

NIH Data Center Disaster Recovery Plan

March 2009

FOREWARD

This Disaster Recovery Plan describes the strategy and procedures for recovering Data Center processing of applications should a disaster substantially disrupt operations.

The plan is organized into three parts: the main body provides a general description of the disaster recovery strategy and program, the appendices provide detailed information for conducting the recovery, and the attachments provide supplemental information. The main body is public information and may be freely distributed; the appendices and attachments contain sensitive information that is restricted to the individuals responsible for recovering Data Center operations. The appendices and attachments must be destroyed when updated versions are received.

The plan is frequently updated to reflect current hardware, software, procedures, applications, and staffing. Revisions are distributed to the disaster recovery team members at least twice a year following the disaster recovery tests.

When copies of the plan are no longer required, please return them to the Disaster Recovery (DR) Coordinator. All corrections are welcome at any time and should be directed to the DR Coordinator.

Adrienne Yang
Disaster Recovery Coordinator

March 31, 2009

TABLE OF CONTENTS

DISASTER RECOVERY PLAN	1
1 INTRODUCTION.....	1-1
1.1 PURPOSE	1-1
1.2 SCOPE	1-1
1.3 DISASTER RECOVERY STRATEGY.....	1-2
1.3.1 Titan and Unix Platforms.....	1-2
1.3.2 NIH email.....	1-3
1.4 DISASTER DEFINITION	1-3
1.5 ASSUMPTIONS	1-3
1.6 AREA-WIDE DISASTERS.....	1-4
1.7 CONTRACTUAL ARRANGEMENT FOR RECOVERY SERVICES.....	1-4
2 DISASTER RECOVERY ACTION PLAN.....	2-1
2.1 BACKUP AND OFF-SITE STORAGE PROCEDURES	2-1
2.2 OFF-SITE STORAGE SERVICES.....	2-1
2.3 DISASTER RESPONSE.....	2-2
2.4 HOT SITE HARDWARE AND SOFTWARE CONFIGURATIONS.....	2-3
2.5 RESUMING NORMAL OPERATIONS	2-4
2.6 SECURITY.....	2-5
3 FUNCTIONAL TEAMS AND RESPONSIBILITIES	3-1
3.1 DAMAGE ASSESSMENT TEAM	3-1
3.2 EXECUTIVE TEAM	3-1
3.3 RESTORATION TEAM.....	3-2
3.4 OPERATIONS TEAM.....	3-2
3.5 CUSTOMER SUPPORT TEAM	3-3
3.6 SALVAGE/RECLAMATION TEAM	3-3
3.7 ADMINISTRATIVE SUPPORT TEAM	3-4
4 TESTING THE TITAN/EOS DISASTER RECOVERY PLAN.....	4-1
4.1 HOT SITE TEST PROCEDURES	4-1
4.2 HOT SITE TEST PLANNING	4-1
4.3 APPLICATION TESTING SUPPORT	4-2
4.4 POST-TEST WRAP-UP	4-2
4.5 HOT SITE TEST SCHEDULE.....	4-3
5 TESTING THE WINDOWS MESSAGING DISASTER RECOVERY PLAN	5-1
6 TRAINING	6-1
7 MAINTAINING THE PLAN.....	7-1

APPENDICES

Appendix A:	Applications and Contact Information
Appendix B:	Directions to Work Area Recovery Center
Appendix C:	Disaster Alert Procedures, Team Members, and Contact Information
Appendix D:	Hot Site Contact Information and Procedures
Appendix E:	Off-Site Storage Contact Information and Emergency Procedures
Appendix F1:	Titan Restore Procedures
Appendix F2:	EOS Restore Procedures
Appendix F3:	Windows Restore Procedures
Appendix G:	Data Communications
Appendix H:	Vendor Contacts
Appendix I:	Contents of the Documentation Box (Doc Box)
Appendix J:	Guidelines for Application Hot Site Tests
Appendix K:	Mainframe Communications
Appendix L:	NIH Electronic Messaging Recovery

ATTACHMENTS

Attachment 1:	Backup Listings
Attachment 2:	Calendars with Julian Dates
Attachment 3:	Hot Site Contract
Attachment 4:	Communications Architecture and Configuration
Attachment 5:	Disaster Recovery Communication Topology
Attachment 6:	Instructions for Completing FedEx Labels
Attachment 7:	z/OS Hardware Configuration
Attachment 8:	Department of the Treasury Payment File Contingency Procedures
Attachment 9:	DHHS Payment Processing Points of Contact

1 Introduction

The Center for Information Technology (CIT) at the National Institutes of Health (NIH) provides information processing services to NIH research and management programs, as well to Department of Health and Human Services (DHHS) and other government agency management programs. CIT also provides networking and telecommunications services to NIH. The information technology equipment supporting these services is housed in the NIH Data Center (the *Data Center*) which is operated by the Division of Computer System Services (DCSS), a component of CIT.

In March 1992 a formal Business Impact Analysis (BIA) of the Data Center's major applications was completed. The resulting disaster recovery plan to mitigate extended interruptions focused on the mainframe, since the major applications were hosted on that platform. Over time, major applications were being hosted on Unix systems and the disaster recovery plan was expanded to include those systems.

As an information technology service provider, DCSS now offers the Disaster Recovery Program as a service to the general customer base. Participation in the disaster recovery program is completely voluntary and is provided on a cost-recovery basis.

1.1 Purpose

This Disaster Recovery Plan documents CIT's Disaster Recovery Program for recovering limited Data Center operations after a disaster. The plan describes the preparation and actions required to effectively respond to a disaster, assigns responsibilities, and describes the procedures for testing and maintaining the plan.

1.2 Scope

The Disaster Recovery Plan is focused only on DCSS-owned and managed computer systems, currently the z/OS mainframe system, Titan, the Unix platforms comprising the EOS system, and the equipment supporting the NIH electronic mail (email) services. This plan addresses all preparation and steps necessary to restore processing on those systems so that the participating applications can continue processing after a disaster has rendered any or all of the systems inoperable.

Many functions and facilities that would be needed in a disaster involving physical devastation are outside the current scope of this plan. These include, but are not limited to:

- care for affected CIT personnel and their families;
- communications equipment supporting the NIH network (NIHnet);
- computing equipment owned by other entities that is housed in the Data Center;
- voice communications internal to CIT;

- ongoing communications protocol between the CIT and NIH officials outside of CIT;
- the role of non-CIT NIH officials following a disaster;
- handling inquiries from the Press;
- implementation of controls to prevent disasters; and
- other aspects of contingency planning such as responses to various localized system outages.

1.3 Disaster Recovery Strategy

1.3.1 Titan and Unix Platforms

Should the Data Center encounter a disaster that prevents it from functioning, DCSS is prepared to provide adequate computational, data storage, and data communications services and facilities at an off-site disaster recovery resource for the participating applications. The off-site disaster recovery resource is a fully operational data center that is prepared to host the NIH systems and participating applications; it is referred to as the *hot site*.

Customers are responsible for disaster recovery preparedness for their applications in the event of a disaster. There is no mandatory requirement that customers use the Data Center's disaster recovery services and facilities. Application owners are free to make other disaster recovery arrangements.

DCSS has assigned a Disaster Recovery Coordinator to oversee the Disaster Recovery Program. The Disaster Recovery Coordinator is responsible for:

- organizing regularly-scheduled, periodic tests of the disaster recovery procedures;
- maintaining and updating the Disaster Recovery Plan based on changes in customer requirements, personnel, hardware and software configurations, and the results of disaster recovery tests and plan reviews; and
- orchestrating the execution of the Disaster Recovery Plan when a disaster has been declared.

DCSS has also designated a Disaster Recovery Technical Support Coordinator for each of the processing systems covered by this Disaster Recovery Program. The coordinators are responsible for:

- assisting the participating application customers in preparing for the disaster recovery test events;
- serving as liaisons for the participating application customers during the disaster recovery tests (by assisting customers in resolving errors in jobs, reporting communications problems to the DCSS disaster recovery team, and answering disaster recovery testing questions in general); and

- assisting the participating application customers in preparing their applications to run successfully at the hot site in the event of a disaster.

DCSS is ready to work with application program managers and technical leaders to further the disaster recovery capabilities of the participating applications. However, it is important that managers of the applications pro-actively prepare their applications for a disaster. This includes participating in the periodic hot site tests and communicating with the Data Center's Disaster Recovery Coordinator regarding significant changes or developments in their applications.

1.3.2 NIH email

DCSS is prepared to provide email services, mailbox storage, and communication at an alternate facility. DCSS will provide the email service in a staged manner. First, email boxes for NIH Institutes and Centers (IC) staff who have been identified as essential employees during Code Red emergencies will be failed over to an alternate location with their historical data. After the identified employees are operational, the plan is to then establish basic email services to the rest of the NIH community. That is, empty mailboxes will be provided; historical messaging data will not be restored for these individuals.

1.4 Disaster Definition

For the purposes of this plan, a disaster is any unplanned event that prevents the Data Center from providing services needed by the participating applications/NIH email for a period of 72 hours or longer. Conditions that could be declared a disaster include, but are not limited to, extended electrical power outage to the computer room, and extensive fire, smoke, water, or explosion damage to computing equipment.

In the event of a disaster, the Damage Assessment Team (reference Section 3.1) will evaluate the damage to the physical assets and functional capability of the Data Center, and report its findings to the Executive Team (reference Section 3.2). The Executive Team will consider the findings together with other available information to make a decision regarding a formal disaster declaration. Only the Executive Team has the authority to declare a disaster.

1.5 Assumptions

The Disaster Recovery Plan has been developed under the following assumptions:

- Only the Data Center is damaged; other buildings on the NIH campus are unaffected.
- Only NIH email and those applications (listed in Appendix A) that are currently participating in the Disaster Recovery Program will be supported.
- A disaster will result in real losses, both for the Data Center itself, and for many of the applications that it supports. At a minimum, time, money, and operational capability will be lost. A physical disaster (hurricane, flood, bomb, etc.) would lead to the loss of at least some data and software.

1.6 Area-Wide Disasters

If the NIH Data Center is adversely affected in an area-wide disaster, the first priority is the well-being of staff members and their families. After the first 24 to 48 hours, the Executive Team (reference Section 3.1) will meet to determine if and when the disaster recovery plan is to be activated. The decision will be coordinated with the NIH Continuity of Operations Plan management team and with owners of the applications participating in the Disaster Recovery Program.

1.7 Contractual Arrangement For Recovery Services

CIT has an Inter-Agency Agreement with the General Services Agency (GSA) for hot site services to accommodate recovery of participating applications for the Titan and EOS systems. The hot site is located in a different geographical region of the continental United States so that it is not susceptible to the same hazards, such as electrical power outages, fire damage, or water damage, that could cause disruptions to the NIH Data Center.

CIT has installed the necessary hardware to support NIH email recovery in HHS space in a Verizon collocation center. The Verizon site is located in a different geographical region of the continental United States so that it is not susceptible to the same hazards that could cause disruptions to the NIH Data Center. CIT has also installed messaging equipment in the local NIH Consolidated Co-Location Site (NCCS) which is not on the same power grid as NIH and is not subject to the same hazards that could cause disruptions to the NIH Data Center.

2 Disaster Recovery Action Plan

2.1 Backup and Off-Site Storage Procedures

Titan:

All disks are dumped to tape on weekly cycles. These weekly dumps are written simultaneously to two separate automated tape libraries (ATLs), one located in the Data Center and the second located in the NIH Consolidated Co-location Site (NCCS). The latter set of tapes are referred to as the *off-site backup tapes*. Both backups are cycled through six sets of tapes so that six successive weeks worth of backups are always maintained.

Incremental backups of all changed data sets are taken daily for public and systems disk storage. Up to five unique backup versions per data set name are maintained. The incremental backups are written simultaneously to the two ATLs. In a disaster situation, all usable tapes will be sent to the hot site.

EOS:

EOS system disks are dumped to tape on weekly cycles and the tapes are rotated to a secure off-site storage facility. The off-site backup tapes are cycled through six sets of tapes. Customer files and data are included in the dumps for those customers who have requested off-site disaster data storage.

Incremental backups of all changed files are taken nightly. The following day the incremental backups are copied to a second tape library located in the NCCS. In a disaster situation, all usable tapes will be sent to the hot site.

NIH email:

The strategy for backing up mailbox data is still being determined.

2.2 Off-Site Storage Services

CIT has contracted with a commercial vendor to provide lockable space (referred to as the NCCS) in a secure, environmentally controlled facility suitable for housing computing equipment. The facility is located in Northern Virginia and authorized CIT staff have 24x7 access.

CIT has contracted with a commercial vendor to provide secure off-site tape storage services. The vendor's facility and procedures meet Department of Defense standards for secure storage. The following services are provided under CIT's contract:

- Delivery of the backup tapes between the storage facility and the Data Center on a weekly schedule;
- Delivery of backup tapes (both those stored at the storage facility and at the NIH campus) to the hot site upon request and as directed by the Data Center (both for disaster recovery tests and for an actual disaster); and
- Delivery of the backup tapes from the hot site back to NIH.

In general, the vendor can respond within two hours notice, twenty-four hours per day, three hundred sixty-five days per year.

Both the NCCS and the off-site tape storage services facility are sufficiently geographically separated from the NIH Data Center such that they are on different power grids to minimize disruption during a Data Center power outage. The two facilities are not susceptible to the same hazards, such as fire damage or water damage, that could cause disruptions to the NIH Data Center.

2.3 Disaster Response

In the event of a disaster, DCSS will take the following actions; responsible teams are indicated:

- Assess the damage to the Data Center to determine if a disaster should be declared. (Damage Assessment Team)
- Make the decision to formally declare a disaster. (Executive Team)
- Establish a Disaster Command Post, if necessary, in another building on the NIH campus having appropriate communications and support equipment. (Executive Team)
- Notify the off-site storage facility, the hot site, key NIH executives, and the participating application sponsors of the disaster declaration. (Executive Team)
- Work with the hot site staff to restore the NIH operating systems and applications at the hot site and establish the communications link to the hot site in preparation for operating at the hot site for the duration of the emergency. (Restoration Team, Operations Team, and Customer Support Team)
- Restore NIH email services at the alternate email processing site in preparation for operating there for the duration of the emergency. (Restoration Team)
- Reconstruct the Data Center. (Salvage/Reclamation Team)
- Conduct operations at the hot site/alternate email processing site until the Data Center is ready to resume operations. (Operations Team, Restoration Team, and Customer Support Team)
- Conduct preparations to leave the hot site and to resume operations at the Data Center. (Operations Team and Restoration Team)

Reference Section 3, Functional Teams and Responsibilities, for details regarding the responsibilities of the disaster recovery teams and the actions required to accomplish the above listed tasks.

2.4 Hot Site Hardware and Software Configurations

The Data Center's standard disaster recovery configuration at the hot site includes a mainframe system, Unix systems, data communications support to the mainframe and Unix systems, and a work area recovery center.

The following are the major hardware components of the standard mainframe configuration:

- IBM processor with sufficient MIPS and memory capacity,
- two logical partitions (LPARs),
- sufficient quantity of tape drives (STK 9840, 3490E, and 3480),
- sufficient disk storage (3390-3 DASD), and
- sufficient printer capacity (IBM 3825-1 page printer, IBM 4245/4248 impact line printer, OCE 372 pagestream with MICR (compatible with IBM 3900), and OCE PS 75 printer (compatible with IBM 3825, 3827)).

The following system software and subsystems will be loaded into the hot site mainframe LPARS as appropriate:

- z/OS operating system,
- Resource Access Control Facility (RACF),
- TSO/ISPF,
- Wylbur under TSO,
- Customer Information Control System (CICS),
- Job Control Language (JCL),
- MODEL 204,
- Limited DB2,
- SPF,
- Transport Control Protocol/Internet Protocol (TCP/IP – TN3270),
- File Transfer Protocol (FTP),
- SAS,
- IMS,
- VISION:Builder and VISION:Report, and
- Connect:Direct.

The following are the major hardware components of the standard Unix configuration:

- AlphaServer 8400 5/625 with sufficient memory capacity,
 - sufficient internal and external disk storage,
 - CD ROM drive,
 - sufficient quantity of tape drives,
 - Laser Jet printer, and
 - network connectivity.
- SunFire V880 UltraSPARC III server with sufficient memory capacity,
 - sufficient internal and external disk storage,

- CD ROM drive,
- tape drive, and
- network connectivity.

The following system software will be loaded onto the hot site AlphaServer:

- Tru64 Operating System,
- Oracle relational database management system,
- Connect:Direct, and
- ADSM.

The following system software will be loaded onto the hot site UltraSPARC server:

- Solaris Operating System, and
- Oracle relational database management system.

Note that at the hot site, the functions of multiple AlphaServers and multiple UltraSparc servers are consolidated into one machine, respectively.

The following are provided to support data communications to the hot site:

- Network Control Center for communication support to the mainframe and Unix computers,
- remote console support for the Unix computers,
- dedicated T1 line with appropriate routers, switches, and firewalls for IP communication between Washington, D.C., and the mainframe and Unix computers, and
- Web redirect services, for Internet connectivity to provide alternate connectivity should the T1 line be inoperable.

The following are the provisions at the work area recovery center, located within driving distance of the Washington, D.C. metropolitan area:

- enough work space to accommodate thirty-two (32) individuals,
- twenty-five work stations,
- twenty-five phone sets,
- twenty-five work stations with 3270 emulation,
- remote consoles for the Unix computers,
- Ethernet connection to the hot site, and
- one facsimile machine and one copier.

DCSS will contract for additional emergency hot site support to meet individual customer's special needs.

2.5 Resuming Normal Operations

While recovery operations are ongoing at the hot site, the Salvage/Reclamation Team will be managing the restoration or rebuilding of the Data Center.

2.6 Security

While operating at the hot site, information security will be assured by firewall restrictions and the security controls on the hot site host systems which will be configured in accordance with the policies and procedures governing the security of the production Titan and EOS systems. As processing continues at the hot site, the hot site host systems will be closely monitored to ensure the systems are not compromised.

The security controls on the messaging servers at the alternate email processing site will be configured in accordance with the policies and procedures governing the security of the NIH production messaging services. While processing in recovery mode, the messaging systems will be monitored to ensure they are not compromised.

3 Functional Teams and Responsibilities

The following subsections describe each functional team's role as well as its responsibilities in preparing for and responding to a disaster. The responsibility for planning, coordinating, and managing this program is assigned to the Disaster Recovery Coordinator with assistance from technical advisors.

The appendices and attachments provide supplemental information and instructions to assist the teams in fulfilling their functions.

3.1 Damage Assessment Team

The Damage Assessment Team assesses the extent of the damage to the Data Center, reports to the Executive Team, and makes a recommendation on declaring a disaster.

The major pre-disaster responsibility is to determine appropriate considerations/criteria for identifying the extent of the damage and the estimated duration of the outage.

The disaster responsibilities and actions are:

- Receive the first alert regarding the disaster.
- Ensure that the NIH police/fire departments have been notified.
- Coordinate with the police and/or fire department to provide for safety, security, and access to the damaged facility.
- Notify the DCSS Director or alternate regarding the potential disaster.
- Assess the damage to each area of the computer facility.
- Brief the Director or alternate, communicating the recommendation(s).

3.2 Executive Team

The Executive Team officially declares that a disaster has occurred, authorizes the execution of the Disaster Recovery Plan, and oversees the execution of the plan during the emergency.

The pre-disaster responsibilities are:

- Approve the DCSS Disaster Recovery Plan and all major or material modifications to the plan.
- Establish primary and alternate disaster command posts, ensuring that the posts are adequately prepared for a disaster.

The disaster responsibilities and actions are:

- Notify the hot site and the off-site storage facility of a possible disaster.
- Review the report of the Damage Assessment Team.
- Declare a disaster:
 - a) establish the command post and communications,
 - b) activate the Functional Teams,

- c) inform the hot site of the disaster declaration, and
- d) initiate the shipment of the backup materials to the hot site.
- Notify the Key Executives (listed in Appendix C).
- Monitor the performance of the Disaster Recovery Teams and the execution and effectiveness of the Disaster Recovery Plan.
- Keep senior CIT management and the designated Information Officer/alternate informed of material/sensitive matters.

3.3 Restoration Team

The Restoration Team brings the hot site/alternate NIH email systems to operational mode by managing the relocation of services to the hot site/alternate email processing site, initiating and managing the recovery procedures at the hot site, and responding to operational problems at the hot site. The Restoration Team also manages the relocation of services back to the Data Center.

The pre-disaster responsibilities are:

- Establish and maintain the recovery procedures for the hot site/email systems.
- Manage and maintain the backup procedures.
- Establish and maintain the disaster recovery data communications link to the hot site.
- Plan and conduct regular hot site/email recovery tests.

The disaster responsibilities and actions are:

- Coordinate recovery procedures with hot site personnel.
- Restore the operating systems environments on the hot site/alternate email processing site host systems.
- Establish the data communications link to the hot site.
- Verify the operating systems and all other system and communication software are working properly.
- Restore the application/mailbox files.
- Support the operations at the hot site by resolving problems and monitoring and maintaining the data communications link to the hot site.
- Support operations at the alternate email processing site by resolving problems.
- Manage the backup tapes that were sent to the hot site.
- Ensure all required backups of the entire system are completed in preparation for leaving the hot site.
- Coordinate the return of the DCSS/customer media to the Data Center.
- Install all NIH system/messaging software at the Data Center.

3.4 Operations Team

The Operations Team assists in the recovery operations and manages the operations of the computer systems at the hot site.

The pre-disaster responsibilities are:

- Ensure that appropriate backups are made on the prescribed, rotating basis and are ready to be taken off-site.
- Maintain current, up-to-date systems operations documentation, ensuring that this documentation is suitably stored off-site.

The disaster responsibilities and actions are:

- Provide assistance to the Restoration Team in the restoration of the system software and customer files, as required.
- Run system and operation jobs, as required.
- Implement and maintain a problem log.
- Provide information to the Customer Support Team regarding the status of the system, operations, and the customer jobs.
- Effect the transfer of media and print output from the hot site to suitable customer pickup location(s).
- Coordinate the shutdown of the hot site operations and the transfer back to the Data Center.

3.5 Customer Support Team

The Customer Support team provides assistance to customers during the disaster from the time the disaster is declared until operations resume at the Data Center.

The pre-disaster responsibilities are:

- Advise and consult with application customers regarding their disaster recovery requirements.
- Assist application customers during disaster recovery tests.

The disaster responsibilities and actions are:

- Notify participating application customers that a disaster has been declared.
- Advise customers of the disaster recovery system status, availability, and accessibility.
- Provide problem diagnosis and resolution guidance/assistance to application owners and their customers.

3.6 Salvage/Reclamation Team

The Salvage/Reclamation Team manages the restoration or rebuilding of the Data Center.

The major pre-disaster responsibility is to maintain current copies of equipment inventory lists, physical plant layout/diagrams (floor plans), and other pertinent documentation describing the DCSS production hardware configuration in a suitable off-site location.

The disaster responsibilities and actions are:

- After the Restoration Team has implemented recovery operations at the hot site, assess the damage to the Data Center and report the damage, with recommendations, to the Executive Team.
- Organize the recovery of salvageable equipment, supplies and the physical plant.
- Initiate, coordinate, and expedite construction and work requests to prepare the NIH facility to receive equipment, supplies, tools, machinery, and utilities (electrical power, telephones, network connectivity, air conditioning, plumbing, water, gas, and HVAC).
- Order and expedite replacements for unusable IT equipment.
- Monitor the construction of the new/repaired facility, and the installation of all utilities and other essentials.
- Monitor the installation of computers, peripherals, and other IT equipment.
- Advise the Executive Team regarding status, progress, and schedules, and any problems associated with the construction/reconstruction and installation.
- Inform the Executive Team when the new/restored facility is ready for use by the participating applications and by other customers.

3.7 Administrative Support Team

The Administrative Support Team provides logistical and organizational support for all the other teams.

The major pre-disaster responsibility is to prepare up-to-date property management lists, inventory lists, and other pertinent documentation on the physical assets of the Data Center, ensuring current copies of this documentation are suitably stored off-site.

The disaster responsibilities and actions are:

- Prepare travel orders and other documents to facilitate the Restore Team activities.
- Provide general administrative support to the Executive Team and to all other DCSS Functional Teams, as necessary.

4 Testing the Titan/EOS Disaster Recovery Plan

Testing and exercising the Disaster Recovery Plan helps to verify that the recovery procedures work as intended and that the supporting documentation is accurate and current. Testing also provides an opportunity to identify any omissions in recovery procedures or documentation and to determine whether personnel are adequately prepared to perform their assigned duties. Therefore, DCSS regularly schedules exercises of its Disaster Recovery Plan at the vendor hot site, referred to as hot site tests (HSTs).

4.1 Hot Site Test Procedures

DCSS schedules two hot site tests per year with sufficient time to test the operating system and customer application recovery procedures. The initial hours are dedicated to exercising the system recovery procedures and establishing the communications link. The remaining hours are dedicated to testing the recovery of participating applications. The hot site tests are managed and conducted by members of the Restoration Team, the Operations Team, and the Customer Support Team, referred to collectively as the *HST Team*.

Prior to the HSTs, the HST Team determines which backup tapes will be used for the tests; establishes a test plan which outlines the HST Team goals and activities for the given test; conducts the necessary preparations for the test; and assists customers in their preparations for the HST. (Customers set their own HST objectives.) During the tests, in addition to providing customer assistance, the HST Team participants maintain a running log of the test activities to assist in the post-test review.

After every test, the HST Team participants meet to discuss the tests in order to improve the recovery procedures and the plan documentation. The HST Team also schedules a meeting with the customers to gain their input and suggestions for improvements.

4.2 Hot Site Test Planning

To ensure a successful hot site test, the HST team will:

- Confirm with the hot site vendor that the hot site mainframe, Unix computer, and data communications configurations will meet the HST needs, and that the hot site will be ready for the test. (Two to three months prior to the scheduled test)
- Set the HST Team objectives for the test and establish action items for the team in preparation for the test. (At least two months prior to the scheduled test)
- Disseminate information to the user community regarding the test. (Six to eight weeks prior to the scheduled test)
- Confirm that preparatory tasks are being completed and review the schedule of events for the days of the HST. (Four to six weeks prior to the scheduled test)

- Discuss the final test preparations with the hot site vendor to confirm the hot site configurations, to obtain the information required for the mainframe backups, and to reconfirm the hot site will be ready. (Two to three days before the scheduled backups for the test will be taken)
- Send the backup tapes and tape lists to the hot site. (One week prior to the scheduled test)

Reference Appendix J for complete guidelines and instructions for preparing and testing applications during a hot site test. This guideline is distributed to the user community well in advance of the HST.

4.3 Application Testing Support

The HST Team offers user support during a hot site test to assist the application owners/participants in successfully running their applications at the alternate site. The assistance includes help with test preparations, on-call support during the duration of the test, resolving reported problems, and serving as the liaison between the user and the HST Team.

Test preparation support includes:

- Ensuring the users have made all appropriate preparations for their data to be available for the HST,
- Ensuring the users are ready for the HST and have no further questions, and
- Ensuring users have the necessary contact phone numbers for user support during the HST.

Hot site test support includes:

- Notifying those users who have not logged on that the disaster system is up and ready for user testing,
- Responding to general user questions and to user problem reports, ensuring they are resolved, and
- Recording all problem reports and general notes to a system status database that is made available to users to read.

4.4 Post-Test Wrap-Up

Two debriefings are scheduled on the days immediately following the hot site test. One is for the HST Team participants to assess the systems software recovery procedures. The second is for the user community who participated in the HST.

These meetings are general discussions to address:

- Areas where the exercise was successful,
- Problems that were encountered, and
- Suggestions for improvements.

Based on the conclusions, an “action list” of improvements to be made prior to the next test is developed and responsibility for implementing them is assigned.

4.5 Hot Site Test Schedule

The bi-yearly tests are scheduled approximately six months apart. To date, twenty-eight tests have been conducted. The next scheduled tests are:

- HST29: July 12 - 14, 2009
- HST30: December 14 - 16, 2009

The following are the dates of the previous tests for the indicated systems:

HST1:	May 3, 1994 – NIH mainframe
HST2:	March 21, 1995 – NIH mainframe
HST3:	September 12, 1995 – NIH mainframe
HST4:	March 14, 1996 – NIH mainframe
HST5:	October 22, 1996 – NIH mainframe
HST6:	May 13, 1997 – NIH mainframe
HST7:	December 12, 1997 – NIH mainframe
HST8:	July 21, 1998 – North and South (consolidation of NIH and HHS mainframes onto two LPARS at NIH)
HST9:	January 22, 1999 – North and South
HST10A:	June 7, 1999 – EOS
HST10:	August 30-31, 1999 – North, South, and EOS
HST11:	February 22-23, 2000 – North, South, and EOS
HST12:	August 14-15, 2000 – North, South, and EOS
HST13:	March 26 - 27, 2001 – North, South, Titan, and EOS
HST14:	November 01 –02, 2001 – Titan (standardized system to replace North and South; hosting North applications at the time of the test), South, and EOS
HST15:	March 26 – 27, 2002 – Titan, South, and EOS
HST16:	November 12 – 13, 2002 – Titan, South, and EOS
HST17:	July 21 – 22, 2003 – Titan, South, and EOS
HST18:	December 8 – 9, 2003 – Titan and EOS
HST19:	July 19 - 20, 2004 - Titan and EOS
HST20:	December 6 - 7, 2004 - Titan and EOS
HST21:	July 18 - 19, 2005 - Titan and EOS
HST22:	December 5 - 6, 2005 - Titan and EOS
HST23:	July 17 - 18, 2006 - Titan and EOS
HST24:	December 4 - 5, 2006 - Titan and EOS
HST25:	July 15 - 17, 2007 - Titan and EOS
HST26:	December 2 - 4, 2007 - Titan and EOS
HST27:	July 15 - 17, 2008 - Titan and EOS
HST28:	December 15 - 17, 2008 - Titan and EOS

5 Testing the NIH email Services Disaster Recovery Plan

The test strategy and procedures are to be determined.

6 Training

In addition to regular testing, team members and managers receive annual refresher training regarding the emergency alert procedures covered in Appendix C and the SunGard notification procedures covered in Appendix D. The following are the completed training sessions:

<u>Date</u>	<u>Training</u>
10/23/06	Manager training regarding emergency alert and SunGard notification procedures
11/2/06	Team member training regarding emergency alert procedures
3/16/09	Manager training regarding emergency alert and SunGard notification procedures

7 Maintaining the Plan

The Disaster Recovery Coordinator of the Data Center is responsible for the maintenance of this document. The plan is updated as needed:

- in response to events such as office moves, telephone number changes, new personnel joining DCSS, retirements, duty changes, and additions or deletions of participating applications;
- after each hot site test to reflect the recommendations resulting from the post-test wrap-up debriefings; and
- after a periodic review of the plan.

As sections of the plan are updated, the revised sections are posted to the internal DCSS web site to ensure the most current information is available to DR team members. DR participants are notified of the changes and are encouraged to produce printouts for their copies of the disaster recovery plan.

Additionally, the plan will be updated in the event an actual disaster occurs. The plan will be reviewed and updated at a convenient point after the initial responses to the disaster have been completed.

Revision History:

<u>Revision Date</u>	<u>Summary of Changes</u>
November, 2000:	The <i>Disaster Recovery Plan</i> , covering the mainframe systems and the <i>Compaq Digital AlphaServer Disaster Recovery Plan</i> were revised following the August, 2000 disaster recovery tests.
July, 2001:	Major restructuring and revision of the disaster recovery plan was completed. The prior two plans are now combined into one plan.
October, 2001	Revised Appendices B, C, D, G, and J due to changes in communications support and the Comdisco contract, and in preparation for the November, 2001 disaster recovery test.
November/December, 2001	Revised main body and Appendices A, C and F following the November, 2001 disaster recovery test.
March, 2002	Revised Appendix J for distribution to customers prior to March, 2002 disaster recovery test.
May 2002	Revised main body and Appendices A, B, C, D, F, G, H, J, K, and L due to contractual changes, customer responses to application surveys, and

results of the March, 2002 disaster recovery test.

June, 2002	Revised Attachments list in table of contents to include Department of the Treasury instructions, and Appendices A, C, D, and, I due to further responses to application surveys, contact information changes, and reviews of procedures.
October, 2002	Revised sections 1, 2, and 4 to reflect contractual changes; Appendix A to reflect changes in applications participating in the Disaster Recovery Program; Appendices B and D to reflect the new work area recovery location; Appendix C to change format and update contact telephone numbers; Appendix F to reflect updates to recovery procedures based upon further reviews; Appendix J in preparation for the November hot site test; and Appendix I to reflect the new location of the Information Security and Awareness Office.
August, 2003	Revised section 1 to clarify user responsibilities; section 4 to record recent test dates; Appendix A to reflect changes to applications supported; Appendix C to reflect personnel changes and to update telephone numbers; Appendix D to reflect changes in vendor support personnel and to update notification procedures; Appendix F to reflect changes to recovery procedures; Appendix G to reflect new IP addresses and update information regarding the T1 line; and Appendix J in preparation for the July hot site test.
April, 2004	Revised sections 1 and 2 to eliminate references to South which was decommissioned January 12, 2004; section 3 to reflect updates to team responsibilities; section 4 to record recent test dates and to describe plan review process and employee training; section 5 to indicate plan approvals; Appendix A to reflect changes to applications supported; Appendix C to reflect personnel changes and updates to alert procedures; Appendix D to reflect changes in vendor support personnel; Appendix F to reflect changes to recovery procedures; Appendix G to reflect changes to IP addresses and pending relocation of the T-1 line; Appendix J in preparation for the December hot site test. Eliminated Appendix L, Hot Site JCL (South) due to the decommissioning of South.
July, 2004	Revised Appendix J and Appendix F in preparation for the July hot site test.
February, 2005	Revised section 2 to update the backup procedures; section 4 to record current test dates; Appendix A to reflect changes to applications supported; Appendix C to reflect personnel changes; Appendix D to reflect changes in vendor support personnel; Appendix E to reflect personnel changes; Appendix F to reflect changes to recovery

	procedures; Appendix G to reflect changes to IP addresses and T-1 line relocation; Appendix H to reflect changes in products and vendor contacts; Appendix J to reflect changes to test instructions prior to the December test.
November, 2005	Revised Section 2 to reflect hot site hardware changes; section 4 to record current test dates; Appendix A to reflect changes to applications supported; Appendices C, D, and E to reflect personnel changes; Appendix F to reflect changes to recovery procedures based on July test results; Appendix G to reflect changes to communications architecture; Appendix H to reflect changes to vendor contact information; Appendix J to reflect changes to test instructions prior to the December test; replaced Attachment 4 (3172 Configuration Controls) with Communication Architecture and Configuration detailing the disaster recovery network (the 3172 is no longer used for communications connectivity on the mainframe).
June, 2006	Revised Appendix J in preparation for the July 17 - 18, 2006 DR test.
July, 2006	Revised Section 1 to clarify the Disaster Recovery Program is provided as a paid service open to any Titan or EOS customer; Section 2 to update the mainframe configuration; Section 4 to record the most current tests; and Section 5 to describe the procedures for publishing plan updates on the DCSS internal web site and to indicate recent revisions. Revised Appendix D to reflect changes to SunGard contact information and DCSS authorized disaster declarers. Revised Appendix F1 to reflect changes to Titan recovery procedures based on July test results. Revised Appendix K to describe Titan communications used for DR testing. This replaces the previous Appendix K, VTAM Telecommunications.
September, 2006	Revised Appendix C to describe mitigation actions to potential accessibility problems to the alternate processing sites, revised team memberships based on personnel changes and updated contact information. Revised Appendix E to indicate the off-site tape backup storage facility is not susceptible to the same hazards affecting the Data Center and to reflect changes in personnel authorized to request tape deliveries and/or manage backup tape storage procedures.
October, 2006	Updated Section 4.5 to include the dates for the July 2007 test. Updated Appendix B to include alternate routes to the work area recovery center. Revised Section 4.6 to include the list of specific training activities and

	frequency.
November, 2006	Updated Appendix C to record personnel and contact changes. Updated Appendix J in preparation for the December DR test. Updated Appendix F1 to reflect changes to the recovery procedures and removal of the ADABAS product.
January, 2007	Updated Section 2.1 to reflect the relocation of the off-site ATL. Updated Section 2.4 to reflect the removal of the ADABAS product. Updated Section 4.1 to remove references to a specific test duration and section 4.5 to reflect completion of hot site test 24 and the date of the 25 th hot site test. Updated Section 4.6 to record completed training sessions.
March, 2007	Updated Appendix H to reflect changes to the list of supported software.
May, 2007	Updated Appendix A to reflect responses to application surveys.
June, 2007	Updated Appendix D to reflect changes to SunGard support personnel. Updated Appendix J in preparation for July test.
October, 2007	Added Section 1.6 to address area-wide disasters. Updated Section 4.5 to record the most recently completed test and to record the date for the future scheduled test. Updated Appendix C, the description of Accessibility to the Hot Site Locations to be consistent with Section 1.6. Updated Appendix F2 to reflect the changes to the recovery procedures based on the July, 2007 test. Updated Appendix J in preparation for the December DR test.
November, 2007	Updated Section 2.2 to include a description of the NIH Consolidated Co-location Site. Updated Appendix C, to reflect personnel changes and contact information changes. Updated Appendix E to include the location, contact number, list of DCSS staff having access to the NCCS, and directions.
March, 2008	Updated Section 1.7 to indicate the alternate processing site is not susceptible to the same hazards as the NIH Data Center. Updated Section 2.2 to indicate the alternate storage sites are not susceptible to the same hazards as the NIH Data Center. Updated Appendix E to include alternate routes to the off-site storage locations. Updated Appendix G to indicate responsibility for fixing T1 line-related problems and to indicate the link is not used for national security emergency preparedness.

April, 2008	Updated Appendix D to reflect changes in SunGard support personnel. Added Appendix F3, Windows Restore Procedures.
May, 2008	Updated Appendix A to reflect responses to application surveys.
June, 2008	Updated Appendix J in preparation for July DR test.
August, 2008	Updated Section 4.5 to record most recent test.
November 2008	Updated Sections 1.2, 1.3, 1.5, 1.7, 2.1, 2.3, 2.6, 3.3 to include information regarding NIH email disaster recovery. Changed the title of Section 4 to indicate the section only describes Titan and EOS DR testing. Added Section 5 to describe NIH email services recovery testing. Changed Section 4.6 to Section 6 since the training will cover all staff involved in Titan, EOS, and NIH email DR. Old Section 5, Maintaining the Plan is now Section 7. Updated Appendix C with Windows messaging restoration team contact information. Updated Appendix J in preparation for the December DR test. Added Appendix L, NIH Electronic Messaging Recovery that describes the email recovery procedures.
March 2009	Updated Section 4.5 to include the most recently completed test date and the future scheduled test dates. Updated Appendix F1 with corrections from the December 2008 test.

Plan Approval:

Revision	Signed, Director DCSS	Date
April, 2004	/s/ John Dickson	4/12/04

Appendix A – Participating Applications and Contact Information

The descriptions of the participating applications include the following information:

- Key contacts,
- Purpose,
- Critical Processing Window(s),
- Software components required by the application for disaster recovery mode processing,
- Data files required for disaster recovery mode processing, and
- Special processing requirements to be accommodated during disaster recovery mode processing.

1 Titan System

1.1 PSC Debt Management System

<i>Contacts</i>	<i>E-mail Address</i>	<i>Office</i>	<i>After Hours (Home/Cell/Pager/Personal email)</i>
David Smith	Dsmith@exchange.nih.gov	301-443-4206	
Mark Goldberg	goldbergm@exchange.nih.gov	301-443-5690	
Bruce Southerland	Bsoutherland@psc.gov	301-443-6611	

Purpose: The Debt Management Collection System (DMCS) supports the collection of money owed to various agencies of the federal government.

Critical Processing Window(s): An outage lasting longer than 12 hours during the work week would have an adverse impact on the function supported by the application.

Software Requirements: CICS; TSO/ISPF; Model 204; SAS; Connect:Direct

Data Storage: Files are stored on CICS03, CICS11, and Disaster Packs.

Special Processing Needs: Treasury Offset Program files are transmitted to the Department of the Treasury over a telecommunications link architected and configured according to Treasury specifications. Connect:Direct is used to effect the transfer. The method for transferring the files in a disaster situation is still being determined by Treasury.

Users access a Wachovia bank Web site to extract and download input to the Debt Management Collection System. DMCS transmits accounting data to UFMS.

Application files are backed up to tape in the Computer Center off-site silo on a weekly basis. The backups would need to be shipped to the hot site in a disaster situation.

1.2 PSC Accounts Receivable System

<i>Contacts</i>	<i>E-mail Address</i>	<i>Office</i>	<i>After Hours (Home/Cell/Pager/Personal email)</i>
David Smith	Dsmith@exchange.nih.gov	301-443-4206	
Mark Goldberg	goldbergm@exchange.nih.gov	301-443-5690	

Purpose: The Accounts Receivable System supports the issuing of bills for medical supplies ordered by federal agencies from the Perry Point, MD medical supply distribution center.

This application is no longer operational; no regular daily processing occurs, but the application is still used for inquiry. The Accounts Receivable System still requires complete Data Center mainframe services including regular backups and disaster recovery services (**but no participation in semiannual tests**). The application is subject to a final SAS 70 audit review after which it will be retired.

The earliest, but not confirmed, cutoff and retirement date is September 30, 2008.

Critical Processing Window(s): None.

Software Requirements: CICS; TSO/ISPF; ADABAS; SAS

Data Storage: Files stored on CICS03, CICS10, ADABAS system volumes, and Disaster Packs.

Special Processing Needs: Application files are backed up to tape in the Computer Center off-site silo on a weekly basis. The backups would need to be shipped to the hot site in a disaster situation.

1.3 PSC ASPER Debt Collection System

<i>Contacts</i>	<i>E-mail Address</i>	<i>Office</i>	<i>After Hours (Home/Cell/Pager/Personal email)</i>
Carol Sery	Csery@psc.gov	301-504-3116	
Mark Goldberg	goldbergm@exchange.nih.gov	301-443-5690	

Purpose: The ASPER Debt Collection System supports the collection of money owed by DHHS employees to DHHS and other organizations.

The function of this application has been replaced by the new payroll system, EHRP. Although there is no regular daily processing against the ASPER Debt Collection System application, it still requires complete Data Center mainframe services including regular backups and disaster recovery services (**but no participation in semiannual tests**).

The projected date for cutoff and retirement is September 30, 2010.

Critical Processing Window(s): None.

Software Requirements: CICS; TSO/ISPF; SAS; VPS printing services

Data Storage: Application files beginning with PRF.CP1 and \$CP1.PRF are stored on CICS11 and DIST01.

Special Processing Needs: None.

1.4 PSC Accounting for Pay System

<i>Contacts</i>	<i>E-mail Address</i>	<i>Office</i>	<i>After Hours (Home/Cell/Pager/Personal email)</i>
John Biggie	Jbiggie@psc.gov	301-443-1588	703-532-1947
Jack Hardland	hardlanj@exchange.nih.gov	301-443-0420	301-476-8161

Purpose: The Accounting for Pay System (AFPS) provides accounting information to DHHS regarding disbursements, expenditures, obligations, and accruals for personnel costs.

Critical Processing Window(s): Every Thursday; the first 5 days of the month; the day the feeder file for the civilian regular payroll run is received (every 2 weeks); the last 5 days of the month when the feeder file for the commission officer regular payroll run is received. An outage lasting more than 24 hours would have an adverse impact on operations during any of these periods.

Software Requirements: TSO/ISPF; Connect:Direct; VPS printing service; Oracle client

Data Storage: All required data sets are located and maintained on DIST01.

Special Processing Needs: AFPS is a distributed application on Titan and EOS (reference 2.2 below). The Titan component receives data from the DHHS Payroll application and the Commissioned Corps Payroll application on Titan, performs preliminary edits on the data and downloads the data to a database on EOS. Batch processes on Titan generate reports (using the information from the EOS database) that are distributed to customer agencies within DHHS.

1.5 PSC Commissioned Corps Payroll System

<i>Contacts</i>	<i>E-mail Address</i>	<i>Office</i>	<i>After Hours (Home/Cell/Pager/Personal email)</i>
Frank Dunn	Fdunn@psc.gov	301-594-0888	301-847-0534
Paul Henderson	Phenderson@psc.gov	301-594-0886	301-384-3318

Purpose The Commissioned Corps Payroll System supports the disbursement of payments to all Active Duty, Retired, and Annuitant Commissioned Officers as well as IHS, NHSC, NSP, and HHSP scholarship recipients. Payments are issued monthly.

Critical Processing Window(s): 10 – 5 working days prior to the last day of the month. An outage lasting more than 24 hours would have an adverse impact on operations during this period.

Software Requirements: TSO/ISPF; SAS; Connect:Direct; MarkIV; Maxbatch; COBOL

Data Storage: All required data sets are located and maintained on DIST01 and DIST02.

Special Processing Needs: The following special forms are printed: Earnings Statements (ASA3) – printed monthly; W2 Statements (ASAW) and 1099R Statements (ASAR) – printed yearly in January to be mailed prior to 1 February. PSC staff orders the forms to be stocked at the NIH Computer Center. These are standard forms that are readily available from the vendor and can be ordered by PSC for shipment to the hot site.

Payment and/or personnel files are transmitted/received to/from the Department of the Treasury, National Finance Center (TSP), and Veterans Administration over telecommunications links architected and configured according to external agency specifications; and payroll information is transmitted to the Social Security Administration (SSA) over a dedicated communications line between NIH and SSA. Connect:Direct is used to effect the transfers.

Backups of the payment and payroll information files are created on 3480 cartridge tapes as part of the regular, monthly production run. In a disaster situation, these tapes would be shipped to Treasury, TSP, and SSA, respectively.

1.6 Federal Drug Administration (FDA) Accounting System (UMBAS)

<i>Contacts</i>	<i>E-mail Address</i>	<i>Office</i>	<i>After Hours (Home/Cell/Pager/Personal email)</i>
Bob Henry	Bhenry1@oc.fda.gov	301-827-2776	301-774-2129
Donna Herbert	donna.herbert@fda.gov	301-827-2778	301-929-3234
Tom Pirring	tpirring@oc.fda.gov	301-827-2787	301-631-5045

Purpose: The FDA Accounting System (UMBAS) provides support for financial control and reporting.

Critical Processing Window: An outage lasting longer than 72 hours during the work week would have an adverse impact on the function supported by the application.

Software Requirements: TSO/ISPF; Connect:Direct

Data Storage: Application files beginning with DFM are maintained on DIST01 and DIST02.

Special Processing Needs: Payment files are transmitted to the Department of the Treasury over a telecommunications link architected and configured according to Treasury specifications.

In a disaster situation, the payment files would be copied to tape, and the tapes would be shipped to Treasury for processing.

Application files are also maintained on tape. Procedures are being implemented to make backups of these tape files to foreign tapes, and to store the backups at the FDA office. The tapes would need to be shipped to the hot site in a disaster situation.

Data is routinely transferred between UMBAS and the Payment Management System on Titan. FTP and the RCVFILE program are used to effect the transfer.

1.7 DHHS Payroll System

<i>Contacts</i>	<i>E-mail Address</i>	<i>Office</i>	<i>After Hours (Home/Cell/Pager/Personal email)</i>
Anita Cobb	acobb@psc.gov	301-504-3093	301-248-2008
Jane Allen	jallen@psc.gov	301-504-3063	301-776-9693
Robert Chichester	rchichester@psc.gov	301-504-3089	202-581-4380
Karen Williams	kwilliams@psc.gov	301-504-3191	540-786-2959

Purpose: The Payroll System provides payroll support services for all DHHS employees ensuring that all T/A (SDA) data is collected, processed, and transmitted to DFAS (Defense Finance & Accounting Systems)..

Critical Processing Window(s): The first Sunday, the first Monday, the first Wednesday, and the second Wednesday of the two week pay cycle. An outage lasting longer than 8 hours during any of these days would adversely impact the function supported by the application, and the timely transmission of any data to DFAS.

Software Requirements: TSO/ISPF; NIH Extended WYLBUR; IMS; Connect:Direct; VPS printing service

Data Storage: Private packs: ESC101, ESC102, ESC103, ESC104, ESC105, ESC106

Special Processing Needs: Time and attendance and pay adjustment data is transmitted to DFAS over the Internet using the host-to-host file transfer product, Connect:Direct.

1.8 NIH Administrative Database

<i>Contacts</i>	<i>E-mail Address</i>	<i>Office</i>	<i>After Hours (Home/Cell/Pager/Personal email)</i>
Jeff Schriver	schriv@mail.nih.gov	301-496-5693	301-963-2243
Carol Perrone	perronec@mail.nih.gov	301-496-1138	703-641-0980
Tony Sambataro	sambatar@mail.nih.gov	301-496-9679	301-916-3533
Richard Rhoads	rhoadsr@od.nih.gov	301-496-1517	

Purpose: The Administrative Database (ADB) supports a broad range of financial and administrative functions at the NIH including the purchase, receipt, and payment of goods and services; payment to NIH fellows; service and supply fund activities; and property management. ADB is an interactive system with some batch functions.

Critical Processing Window(s): An outage lasting longer than 72 hours during the work week would have an adverse impact on the function supported by the application.

Software Requirements: TSO/ISPF; NIH WYLBUR; DB2; IMS; Connect:Direct; Connect:MAILBOX; VPS printing service

Data Storage: Private packs: ODA103, ODA104, ODA105, ODA106

Special Processing Needs: Payment files are transmitted to the Department of the Treasury over a telecommunications link architected and configured according to Treasury specifications. Connect:Direct is used to effect the transfers. In a disaster situation, the payment files would be copied to tape, and the tape would be shipped to Treasury.

Purchase card information files are transmitted from First Bankshares to Connect:MAILBOX using a dial-in connection.

A SILK Web interface provides user access to reports created by ADB batch processing. In a disaster situation, the reports could be printed and distributed to users.

Every business evening disksave tapes are made of the four ADB private packs. The saves are created and stored in the Titan off-site ATL. In the event of a disaster, a determination would be made regarding where the most current private pack backups are located. The private packs would be restored from the most current backup tapes.

1.9 NIH Central Accounting System

Contacts	E-mail Address	Office	After Hours (Home/Cell/Pager/Personal email)
Maria Sotto	sottom@mail.nih.gov	301-594-6278	301-675-7064
Jeff Schriver	schriv@mail.nih.gov	301-496-5693	301-963-2243
Carol Perrone	perronec@mail.nih.gov	301-496-1138	
Richard Rhoads	rhoadsr@od.nih.gov	301-496-1517	

Purpose: The Central Accounting System (CAS) is a fully-automated double-entry accounting system supporting the accounting transactions incurred in the operations of NIH. CAS is a strictly batch processing system.

Critical Processing Window(s): An outage lasting longer than 48 – 72 hours at any given time would have an adverse impact on the function supported by the application.

Software Requirements: TSO/ISPF; NIH WYLBUR; IMS

Data Storage: Private packs: OFM101, OFM102.

Special Processing Needs: The ADB creates two datasets of accounting transactions each batch processing day (Monday through Friday) that are processed by CAS the same day. CAS also reads four of the ADB IMS databases, as well as gathering accounting transactions from

other sources including Grants (Information for Management, Planning, Analysis and Coordination System - IMPAC), Payment Management System (PMS), Central Payroll System, NIH subsystems, manual entries from the Office of Financial Management, and the Rotating Error File (with corrections and deletions).

CAS creates transactions for updating other Department systems including Payment Management System. CAS files are transmitted to the NIH Business System (NBS) and the Data Warehouse.

Every business evening, disksave tapes are made of the two CAS private packs. The saves are created and stored in the Titan off-site ATL. In the event of a disaster, a determination would be made regarding where the most current pack backups are located. The private packs would be restored from the most current backup tapes.

1.10 Nuclear Regulatory Commission License Tracking System

<i>Contacts</i>	<i>E-mail Address</i>	<i>Office</i>	<i>After Hours (Home/Cell/Pager/Personal email)</i>
Mallory Green	MMG@nrc.gov	301-415-7277	703-922-6077
David Offutt	dko@nrc.gov	301 415-5906	
Jim Parker	JSP@nrc.gov	301-415-5853	
Menelik Yimam	MGY1@nrc.gov	301-415-0200	
Michael Daley	MED1@nrc.gov	240-753-0228	
Bruce Johnson	BAJ2@nrc.gov	240-753-0217	

Purpose: The License Tracking System enables the Nuclear Regulator Commission's Office of Nuclear Material Safety and Safeguards (NMSS) to increase control, standardization, and productivity of the licensing process.

Critical Processing Window(s): An outage lasting longer than 24 hours during the work week would have an adverse impact on the function supported by the application.

Software Requirements: TSO/ISPF; NIH Extended WYLBUR; COBOL/370 V1R1; CA-RAMIS (installed on NRC private packs)

Data Storage: Private packs: NRC101, NRC102, NRC103, NRCI13, NRCI14, and NRCI15

Special Processing Needs: The NRC runs nightly backups of their private packs, 5 nights per week. The tapes are produced and stored in the NIH Data Center.

In the event of a disaster, a determination would be made regarding where the most current private pack backups are located. The NRC private packs would be restored from the most current backup tapes.

2 EOS

2.1 DHHS Payment Management System

<i>Contacts</i>	<i>E-mail Address</i>	<i>Office</i>	<i>After Hours (Home/Cell/Pager/Personal email)</i>
Bob Bessio	bbessio@psc.gov	301-443-9213	301-774-7932 bbessio@erols.com
Mathew Matsuda	mmatsuda@matsudainc.com	703-499-9477	703-497-0193 home 703-577-6520 cell

Purpose: The DHHS Payment Management System (PMS) is a centralized financial system supporting the payment of funds to recipients of grants awarded by DHHS Agencies and several other Federal agencies that DHHS cross-services.

Critical Processing Window(s): 24 hours/ 7 days a week on dedicated processors: lapis, garnet

Software Requirements: EOS: Oracle RDBMS, Oracle PL/SQL, Oracle OAS; Connect:Direct
Titan: Connect:Direct

Data Storage: Oracle RDBMS instance: pmsprod
Oracle Application server instance: pmspoas

Special Processing Needs: PMS is a distributed application executing on two dedicated AlphaServers and on Titan. One AlphaServer hosts the database and the second server processes user access requests to the database. Titan serves as a front-end for transferring data between the PMS database server and external entities. The PMS AlphaServers are protected by a dedicated firewall.

A Web front-end hosted on a server located in the DHHS Rockwell site serves as external users initial interface to PMS. The Web front-end is connected to NIHnet by a dedicated link. A backup web server is in place at NIH/CIT Customer Server Area 2 (CSA2). The primary web server is being relocated to the CSA2 (estimated completion, March 31, 2007).

The PMS application will be restored on two dedicated AlphaServers at the hot site and will be protected by a firewall at the hot site. The DCSS contract for emergency hot site support includes the following configuration to support PMS:

- Two AlphaServers, each with sufficient memory capacity,
 - sufficient internal and external disk storage,
 - system console,
 - CD-ROM drive,
 - cartridge tape drive,
 - LaserJet printer, and
 - network connectivity.
- A Cisco firewall configured with appropriate rule sets to restrict traffic to the two Alphaservers.

2.2 PSC Accounting for Pay System

<i>Contacts</i>	<i>E-mail Address</i>	<i>Office</i>	<i>After Hours (Home/Cell/Pager/Personal email)</i>
John Biggie	Jbiggie@psc.gov	301-443-1588	703-532-1947
Jack Hardland	hardlanj@exchange.nih.gov	301-443-0420	301-476-8161

Purpose: The Accounting for Pay System (AFPS) provides accounting information to DHHS regarding disbursements, expenditures, obligations, and accruals for personnel costs.

Critical Processing Window(s): Reference section 1.4 above.

Software Requirements: Oracle (basic, plus import, export, sql-loader); SQL*NET; secure shell; secure FTP, Connect:Direct, Forms and Reports.

Data Storage: The following are the high level AFPS application and database directories:

- ***AFPS Production***
 AFPSP on EOS Database binaries: /orabin/dfo-afps/afpsp
 Database files: /oracle/dfo-afps/afpsp
 AFPSPIAS on Polaris Middle Tier binaries: /oramount/orabin/dfo-afps/afpspias
 Middle Tier ApplicationData: /oramount/oracle/dfo-afps/afpspias
- ***AFPS Training***
 AFPST on EOS Database binaries: /orabin/dfo-afps/afpst
 Database files: /oracle/dfo-afps/afpst
 AFPSTIAS on Polaris Middle Tier binaries: /oramount/orabin/dfo-afps/afpstias
 Middle Tier Application Data: /oramount/oracle/dfo-afps/afpstias
- ***AFPS Development***
 AFPSD on EOS Database binaries: /orabin/dfo-afps/afpsd
 Database files: /oracle/dfo-afps/afpsd
 AFPSDOAS on Polaris Middle Tier binaries: /oramount/orabin/dfo-afps/afpsdoas
 Middle Tier Application Data: /oramount/oracle/dfo-afps/afpsdoas

Note: The production and test environments will become similar to development after the upgrades.

Special Processing Needs: AFPS is a distributed application on Titan and EOS (reference section 1.4 above). The database is hosted and maintained on EOS. Users access the data through a Web interface (forms hosted on a Sun Server).

2.3 Administration for Children and Families (ACF) GATES

<i>Contacts</i>	<i>E-mail Address</i>	<i>Office</i>	<i>After Hours (Home/Cell/Pager/Personal email)</i>
Deborah Ferrenz	dferrenz@acf.hhs.gov	202-690-7044	301-588-7531 home 240-463-4928 cell; 2404634928@mms.att.net for text emails to cell phone dferrenz@comcast.net
Paul Hasz	phasz@acf.hhs.gov	202-690-7037	301-934-0600 home 202-255-6005 cell phasz@comcast.net
David Jenkins	djenkins@acf.hhs.gov	202-690-5802	304-876-1539 home 703-627-9102 cell
Natalya Grimberg (tester only)	ngrimberg@acf.hhs.gov	202-205-3449	

Purpose: GATES supports the distribution of the various ACF grants to state, local, tribal, and non-profit organizations. It also supports grants for AOA, IHS, HRSA, OS/OPHS and discretionary grants for CMS (although CMS's are not transmitted to UFMS).

Critical Processing Window(s): An outage lasting longer than 48 hours during the last two weeks in September would adversely impact the function supported by GATES.

Software Requirements: EOS: Oracle (basic, plus import, export, sql-loader); SQL*NET; telnet or secure shell; FTP and secure FTP, *Connect:Direct* (no longer critical)

Titan: TSO/ISPF; *Connect:Direct*; VPS printing (none of these are critical)

Data Storage: EOS: All files and directories are under /usr/users/gates/bin and /usr/users/gates/disaster

Special Processing Needs: GATES is a distributed application executing on EOS. EOS hosts the database and Titan no longer serves as a front-end for transferring data between EOS and external entities. Titan is used only to download non-critical PMS data.

Grant transaction files are transferred from EOS by SFTP to the HHS UFMS server using public key/private key security and this connection is essential to the awarding of grants. If connectivity were unavailable, the files could conceivably be transferred using e-mail, but it would be preferable to set up connectivity between the NIH DR site for EOS and UFMS.

UFMS (the HHS Accounting system) relays the payment transactions to the Payment Management System. UFMS management has determined that in no circumstances should UFMS be bypassed in favor of sending transactions directly to PMS. In the event that a disaster lasted for weeks, ACF has an agreement that UFMS would load a quarterly transaction file that had already been sent and saved at UFMS for this purpose.

GATES also collects files from UFMS using the same SFTP method and from PMS (using Connect:Direct but FTP could be substituted). These are not time-critical; GATES can function for at least a week without them. In the event of a disaster, ACF could arrange to have UFMS or PMS send the files on diskette or tape or by e-mail.

Biweekly, the HHS personnel system writes a file to VVG1FWA on Titan; the file is collected on EOS (using Connect:Direct) for input to GATES. This is not a time-critical function. In the event of a disaster, GATES supports a manual method for inputting any essential personnel data.

ACF manages a Web application, On-line Data Collection (OLDC), which uses another Oracle database hosted on servers located in the Aerospace building in Washington, DC. Information is exchanged between OLDC and GATES using Oracle database links (SQL*NET TCP protocol) to transmit data between Oracle databases hosted on each system. If the Aerospace database is restored elsewhere, the ACF database administrator will have to modify the database link definition at the disaster site in order for GATES to function. If the Aerospace database is unavailable and is not restored elsewhere, the ACF database administrator will have to make a few changes to GATES objects in the NIH database to turn off the linkages in order for GATES to function.

2.4 ACF TANF

<i>Contacts</i>	<i>E-mail Address</i>	<i>Office</i>	<i>After Hours (Home/Cell/Pager/Personal email)</i>
Arianta Anaya	aanaya@acf.hhs.gov	202-401-5592	703-599-1237 (Cell)
Gary Cochran	gcochran@acf.hhs.gov	202-401-6465	301-938-1794 (Cell)
Paul Hasz	phasz@acf.hhs.gov	202-690-7037	

Purpose: TANF supports the data collection and processing of Temporary Assistance for Needy Families (TANF) and Separate State Program for Maintenance Of Effort (SSP-MOE). TANF receives data from state or tribal entities. TANF consists of several components - FTDRS, HPBS and TDRS.

Critical Processing Window(s): An outage lasting longer than 24 hours after the daily cronjob is run Monday through Thursday, or Saturday would adversely impact the FTDRS component.

Software Requirements: EOS: Oracle (basic, plus import, export, sql-loader); SQL*NET; PL/SQL; telnet or secure shell; FTP or secure FTP

Titan: TSO/ISPF; Connect:Direct; VPS printing

Data Storage: EOS: All files and directories are under /usr/users/tanf/disaster

Titan: All data files, JCL, and CLISTs under the ADS.E2J. directory. Data files received are backed up to tapes.

Special Processing Needs: The Final TANF Data Reporting System (FTDRS) is a distributed application executing on Titan and EOS. Titan serves as the front-end for receiving data from

state and tribal entities, either via Connect:Direct or secure FTP. The states electronically transmit the files directly to Titan and the tribes submit their files as email attachments to ACF where the data is examined for quality control purposes and the data is then submitted from ACF to Titan. States and tribes can submit selected information to TANF via the Internet.

EOS serves as the back-end to perform most of the FTDRS processing. A daily cronjob initiates shell scripts and C programs that download TANF and SSP-MOE data from Titan to EOS, process the data, indicate errors that may exist, and populate the Oracle database. The cronjob runs at 5 PM, Monday through Thursday and 6 AM on Saturday. The data received from the states or tribes should be processed on the same day or the following day. The data received from the states is backed up to cartridge tape on the day following receipt and retained in the NIH Data Center for 180 days. In the event of disaster, and the backup tapes are unusable, and prior data is required, it can be requested from the states and tribes since they maintain backups of previously submitted data.

The High Performance Bonus System (HPBS) is also a distributed application executing on Titan and EOS. Titan serves as the front-end for receiving data from states, either via Connect:Direct or secure FTP. Four times a year HPBS performs comparisons of selected TANF data with the Office of Child Support Enforcement's (OCSE) National Directory of New Hires (NDNH) database located at the Social Security Administration National Computer Center. Connect:Direct is used to initiate JCL on the OCSE system. The OCSE JCL retrieves TANF data from Titan, performs the comparison, and transmits the results back to Titan. This process uses the direct link between NIH and SSA. In a disaster situation, the schedule could be altered if necessary; this is not a time sensitive process.

EOS serves as the back-end to perform most of the HPBS data processing. HPBS requires manual intervention rather than cronjobs to initiate processing. The data file processed is backed up to cartridge tape and retained in the NIH Data Center for 180 to 360 days. In the event of disaster, and the backup tapes are unusable, and prior data is required, it can be requested from the states and tribes since they maintain backups of previously submitted data.

The TANF Data Reporting System (TDRS) is a TANF web based application. TDRS is hosted on web servers located in the Aerospace building in Washington, DC. A cronjob runs daily to synchronize the information between the ACF's Oracle database and Web servers.

2.5 PSC Enterprise Human Resources and Payroll

<i>Contacts</i>	<i>E-mail Address</i>	<i>Office</i>	<i>After Hours (Home/Cell/Pager/Personal email)</i>
Richard Butler	richard.butler@psc.hhs.gov	301-504-3112	301-390-1338 (H), 301-343-2720 (C)
Jonathan Welbon	jonathan.welbon@psc.hhs.gov	301-504-3073	301-248-2008 (H), 301-529-6095 (C)

Purpose: The Enterprise Human Resources and Payroll (EHRP) supports processing of Departmental human resource activities and reporting, ensuring that the requisite changes are properly reflected and processed by the Departmental Payroll system. The EHRP functions are currently initiated through the use of a PeopleSoft/Oracle Human Resources application. The current end-user base is the Departmental management personnel and Human Resource

community. PSC/HRS/EAD operations personnel are responsible for application maintenance and interface activities.

Critical Processing Window(s): Peak Processing activities occur on a biweekly cycle based on the Departmental payroll cycle. The key processing window occurs for five (5) days from Wednesday prior to the end of the pay cycle through Sunday (pay periods end on Saturday). The pay period end dates for 2005 are: 1/8, 1/22, 2/5, 2/19, 3/5, 3/19, 4/2, 4/16, 4/30, 5/14, 5/28, 6/11, 6/25, 7/9, 7/23, 8/6, 8/20, 9/3, 9/17, 10/1, 10/15, 10/29, 11/12, 11/25, 12/10, 12/24. An outage of 8+ hours would severely impact user ability to complete work on time, and the ability of operations personnel to complete payroll interface activities. During the other periods of the cycle, an outage of 2-3 days could be dealt with.

Software Requirements: Oracle (basic, plus import, export); SQL*NET; secure shell; secure FTP, Connect:Direct/Secure+

Data Storage:

- **racer (database)**
/opt/app/oracle – Oracle binaries and creation scripts/data (4GB)
/u01/oradata/* - /u15/oradata/* - 10 GB each
/u16/oradata/* - /u19/oradata/* - 25 GB each
- **coral and viper (Application and Web Server portion restored to single host configuration)** (20 GB)
Includes application (PeopleSoft) software, configuration, and data

Special Processing Needs: The EHRP application is hosted on multiple dedicated HP servers. At the hot site, the multiple servers will be restored to a single HP system. The DCSS contract for emergency hot site support includes the following configuration to support EHRP:

- HP9000-N400 with sufficient memory capacity,
- sufficient internal and external disk storage,
- DVD-ROM drive,
- cartridge tape drive,
- LaserJet printer,
- remote console, and
- network connectivity.

EHRP transmits payroll information over the Internet to the Defense Financing and Accounting Service (DFAS) mainframe site in Mechanicsburg, PA, which issues salary payments to DHHS employees. Connect:Direct/Secure+ is used to effect the transfer.

2.6 NIH New Business System

Contacts	E-mail Address	Office	After Hours (Home/Cell/Pager/Personal email)
Carole Perrone	perronec@mail.nih.gov	301-496-1138	301-775-6396
Surya Chunduru	chunduru@mail.nih.gov	301-435-6568	240-899-9923

Purpose: The New Business System (NBS) project is a replacement of all administrative functions currently supported by NIH legacy systems on the mainframe, including procurement and contracting, travel, property, inventory, central accounting, accounts payable and receivable, and service and supply fund (working capital fund) activities. NBS serves several thousand NIH employees.

NIH selected Oracle's Enterprise Resource Planning Applications and "bolt-on" products from Compusearch, Gelco, and Sunflower as the foundation of a new business/administrative IT system. The first two modules of the NBS have now been deployed, accepted, and are officially part of the system of records at NIH. Gelco's Travel Manager and the Oracle Travel Manager Interface were deployed in September, 2003. Oracle's General Ledger, Federal Administrator, and components of Accounts Payable/Receivable were officially deployed October 1, 2003. Further financial modules and others for acquisition (Oracle Purchasing, iProcurement, and Warehouse Manager, and Compusearch Prism) and for Property (Sunflower) are now well along in the design stages. A module that will address working capital fund components will follow.

Critical Processing Window(s): An outage lasting longer than 72 hours during any time of the week, would have an adverse impact on the functions supported by NBS. This timeframe is based on the current ADB requirements. Any unavailability of the NBS during the core business hours, 7:00 am to 6:00 pm, Monday through Friday, as well as during the times listed in the table below, would cause a severe impact on NBS operations.

Task Description	Concurrent Program/Set/Process	Frequency	Start
Database Cold Backup	A158PROD backup	Saturday	19:00
Database Cold Backup	G816PROD backup	Saturday	19:00
Database Cold Backup	C500PROD backup	Saturday	19:00
Database Cold Backup	S380PROD backup	Saturday	19:00
Database Cold Backup	M551PROD backup	Saturday	19:00
Gather Schema Statistics	Gather Schema Statistics	Sunday	04:00
Extract data from Legacy Warehouse Datamarts; transform/load into nVision Data Warehouse	nVision ETL Process	Tue - Sat	02:01
Extract data from Oracle Apps and Gelco Travel Manager Databases; transform/load into nVision Data Warehouse	nVision ETL Process	Mon - Fri	19:00
Core financials extract - from Oracle Applications database	nVision ETL Process	Mon - Sat	06:15
Export of People data from Oracle HR tables to Oracle Vendor tables; export of People data to Gelco Traveler tables	NIHTM Import Patient as Traveler and Vendor	Every 4 minutes after completion of prior run	24:00
Import TMRPP Transactions into AP	NIHAP Payables Open Interface Import	Every 5 minutes	24:00
Import of Organizational data into Oracle Apps from file received from HRDB ADMCD table	NIHMM Organization Maintenance Interface (Report Set)	Daily	01:45
GL Optimizer	Program - Optimizer	Daily	02:30
Post VALTRANs and Send Balance of	NIHGL Valtran Posting and DW Balance	Mon - Sat	03:00

Task Description	Concurrent Program/Set/Process	Frequency	Start
Accounts files(FSGs) to DW	of Accounts (Report Set)		
PRC: Update Project Summary Amounts	PRC: Update Project Summary Amounts	Daily	03:00
Post VALTRANS in GL	Automatic Posting	Mon - Fri	03:00
FSG 1	Run Financial Statement Generator	Tue - Sat	04:20
FSG 2	Run Financial Statement Generator	Tue - Sat	04:20
FSG 3	Run Financial Statement Generator	Tue - Sat	04:20
FSG 4	Run Financial Statement Generator	Tue - Sat	04:20
Import TRAVEL Invoices into AR	NIH Autoinvoice Master Program	Daily	06:00 & 16:00
Import Clinical Center Patient data into Oracle Apps from files received from NED and HRDB NIHMAST table	NIHMM People Interface (Report Set)	Daily	07:00
NIHTM Send Incomplete POs	NIHTM Send Incomplete POs to Emails	Mon - Fri	07:00
Import of ACH information for People into Oracle Apps from file received from ADB	NIHAP_ACH_INTERFACE_PROCESSES (Report Set)	Mon - Fri	07:30
Import TMADV, TMINV, TMUSB, TMIAD, TMDM Transactions; run Payables Accounting Process	NIHAP Invoice Imports And Payables Accounting Process (Request Set)	Mon - Fri	16:00
Interfaces -> NIHAR: General Ledger	NIHAR: General Ledger	Mon - Fri	16:00
NIHFV Budget Execution Transfer to GL	NIHFV Budget Execution Transfer to GL (Report Set)	Daily	17:00
NIHFV Federal Vertical Transfer to GL	NIHFV Federal Vertical Transfer to GL (Report Set)	Mon - Fri	17:00
Create accounting entries for Payable documents	Payables Accounting Process	Daily	17:20
Project/Expenditure CAN Maintenance and Feed to ADB	NIHGLPA Maintain CANS and Feed to ADB (Report Set)	Mon - Fri	18:00
Post the multiple journal batches in GL	Automatic Posting	Mon - Fri	18:00
Journal Import for Source 'TRAVEL'	NIHGL Submit Journal Import	Daily	18:00
Set Default Job Code for Patients/NON-NIH Affiliates	NIHMM Set Default Job Code for Patients/NON-NIH Affiliates	Daily	19:00
Send Oracle Sub-ledger data to DW	NIHGL General Ledger to Valtran Interface Report Set	Mon - Fri	20:00
Check Fed Admin Appropriations, Apportionments and Allotments	NIHGL_FV_BUDGET_CHECK	Mon - Fri	20:00
PRC: Interface Supplier Costs	PRC: Interface Supplier Costs	Daily	22:00
NIHGL General Ledger to Valtran Interface	NIHGL General Ledger to Valtran Interface	Mon - Fri	22:00
NIHGL CAN/ACCS file to DW	NIHGL CAN/ACCS file to DW	Mon - Fri	23:00
NIHGL Gelco Travel Data to DW	NIHGL Gelco Travel Data to DW	Mon - Fri	23:00
NIHGL SGL Mapping to DW	NIHGL SGL Mapping to DW	Mon - Fri	23:00
Export from Gelco of Travel Order information specific to CSR travel	CSR Interface	Tue - Sat	04:20
NIHGL TRANSCODE Mapping to DW	NIHGL TRANSCODE Mapping to DW	Mon - Fri	23:00
NIHGL VEND_CUST Data to DW	NIHGL VEND_CUST Data to DW	Mon - Fri	23:00
NIHGL VALTRAN Daily Process Set (Report Set)	VALTRAN INTERFACE: CAS to GL to DW	Mon - Fri	23:51
Review Project Approval Workflow	N/A	Daily	
ADI Budget Loads		As needed	
PO Import Process		Immediate	
Gelco: Load Per Diem Rates		As needed	Manual
Gelco: Archive Documents		As needed	Manual

Task Description	Concurrent Program/Set/Process	Frequency	Start
Cash Mgmt Interface	NIHCE Load Staging Table from GTE file (Report Set)	Monthly	Manual
Send Email to OFM of Treasury Confirmation		Mon - Fri	Manual
Non FTE Workflow	Non FTE Workflow	N/A	N/A
CD Jobs PUSH: CAN.MAINT PUSH: MOD.VALTRAN PUSH: CSR PUSH: TREASURY PULL: TREASURY PULL: NED PULL: ACH PULL: NIHMAST PULL: VALTRAN		Mon - Fri	

Software Requirements:

- **Danica**
SunOS 5.9
Java 1.3.1, Java 1.4.2, unzip 5.42, zip 2.3, gtar 1.13
SSH, SFTP
- **Andretti**
SunOS 5.9
Java 1.3.1, Java 1.4.2, unzip 5.42, zip 2.3, gtar 1.13
SSH, SFTP
- **Andromeda**
SunOS 5.10
Java 1.4.2, Java 1.5, unzip 5.42, gzip 1.3.3, gtar 1.13
SSH
- **Zinc**
Tru64 V5.1B
Java 1.3.1, Java 1.4.2, unzip 5.42, zip 2.3, gtar 1.13
SSH, SFTP
- **Compusearch**
Windows 2003 SP4
IIS Web Server 5
Merrant ODBC Driver 3.0
Oracle ODBC Driver 8.01
Microsoft ODBC Driver for Oracle 2.57
Export Jobs 1.7.6
Compusearch Application 5.0 SP29
OCI Component FAC 6401-20
Application Code Logic (PL/SQL) 9.2.0.7

Database Oracle Home 9.2.0.7
Microsoft SOAP Toolkit 3.0
Loftware 6.1.2.5

- **Loftware**
Windows 2003 SP4
Loftware 9.1.2.3
Oracle Client 9i
JDK 1.4.2.10
Loftware Connector 2.6.2.11
- **Titan**
SSH, SFTP

Data Storage:

- **Danica**
/oraappl/od-nbs/a159prod
/oraappl/od-nbs/s380prod
/oraappl/od-nbs/c500prod
/oraappl/od-nbs/iappprod
/oraappl/od-nbs/backups
/oraappl/od-nbs/staging/dbarep/scripts
/var/opt/oracle
- **Andretti**
/oraappl/od-nbs/a159prod
/oraappl/od-nbs/s380prod
/oraappl/od-nbs/m551prod
/oraappl/od-nbs/backups
/oraappl/od-nbs/staging/dbarep/scripts
- **Andromeda**
/oraappl/od-nbs/w133prod
/oraappl/od-nbs/staging/dbarep/scripts
- **Zinc**
/oraappl/od-nbs/g816prod
/oraappl/od-nbs/igelprod
/oraappl/od-nbs/backups
/var/opt/oracle

Special Processing Needs: The NIH NBS application is hosted on multiple dedicated UNIX systems (AlphaServers and Sun servers). At the hot site, the application will be consolidated onto fewer servers. The DCSS contract for emergency hot site support includes the following configuration to support NIH NBS:

- One AlphaServer with sufficient memory capacity,
 - sufficient internal and external disk storage,
 - CD-ROM drive,
 - cartridge tape drive,
 - LaserJet printer,
 - remote console, and
 - network connectivity.
- Three Sun servers with sufficient memory capacity,
 - sufficient internal and external disk storage,
 - CD-ROM drive,
 - tape drive,
 - remote console, and
 - network connectivity.
- Two Windows servers with sufficient memory capacity,
 - sufficient internal and external disk storage,
 - DVD-ROM drive,
 - remote terminal connection, and
 - network connectivity.

All file transfers between the NBS and external systems are managed through an encrypted channel using SFTP or by tunneling Secure Shell (SSH) through a proxy server (drandromeda). The only system presently connecting to the production NBS via SSH tunnel is the nVision project (indus.cit.nih.gov:137.187.65.26); the access is limited to read-only.

Payment files are transmitted from Titan to the Department of the Treasury over a telecommunications link architected and configured according to Treasury specifications. Connect:Direct is used to effect the transfers. In a disaster situation, the payment file will be created on a tape to be shipped to Treasury.

The following Titan SSH/SFTP accounts are required:

BHX1ENC
 BHX1DHI
 BHX1XVQ

2.7 NIGMS Database

<i>Contacts</i>	<i>E-mail Address</i>	<i>Office</i>	<i>After Hours (Home/Cell/Pager/Personal email)</i>
Jose Lopez (ISDS Chief)	lopezj@nigms.nih.gov	301-594-2680	
Faustina Ifedi	ifedif@nigms.nih.gov	301-594-2680	

Purpose: The NIGMS database contains information used in the administration of NIGMS grants. Some of the data is copied from the IMPACII database, and some of the data is NIGMS specific and is stored only in the NIGMS database. The IMPACII data is copied daily to the

production database and weekly to the development database mainly using PowerBuilder Data Pipe, or Snapshots for downloading smaller tables.

The NIGMS database is accessed by NIGMS employees through the NIGMS Extramural Support System (NESS) and the NIGMS Administrative Support System (NASS). Both systems are part web-based, running on NIGMS servers, and part client/server, running from NIGMS network servers and user machines.

Critical Processing Window(s): The most critical processing time having a severe impact on users' abilities to get their jobs done is during the month prior to, and including, the NIGMS Council meetings, and the four weeks prior to and following the end of each fiscal year (Sept. 30). The NIGMS Council meets three times a year: January, May, and September. The maximum length of time the database could be unavailable during the critical processing times before causing a severe impact on user operations would be approximately four days.

Software Requirements: Oracle

Data Storage: The four database instances are: NIGMSP (GMP), NIGMSD (GMD), NIGMST (GMT), and NIGMSPUB (GMPUB)

Special Processing Needs: None.

2.8 NIH Electronic Research Administration

<i>Contacts</i>	<i>E-mail Address</i>	<i>Office</i>	<i>After Hours (Home/Cell/Pager/Personal email)</i>
Ali Ghassemzadeh	ghassema@mail.nih.gov	301-435-0981	
Nora Hermida	hermida@mial.nih.gov	301-435-4470	

The Office of Extramural Research (OER) is responsible for the Electronic Research Administration (eRA) application which runs on multiple OER servers housed in the data center customer server area and on multiple host systems managed by DCSS.

The DCSS contract for emergency hot site support includes multiple host systems to support both OER servers and DCSS managed servers. The following configurations support the OER servers:

The following configurations support the DCSS-hosted servers:

- Two Sun Fire 280R servers with sufficient memory capacity,
 - sufficient internal and external disk storage,
 - CD-ROM drive,
 - tape drive,
 - remote console, and
 - network connectivity.

Appendix B – Directions to Work Area Recovery Center

The SunGard Washington-Baltimore Work Group Recovery Facility is located at:

505 Huntmar Park Drive
Suite 100
Herndon, VA 20170

Telephone Number: (703) 326-4900; (888) 815-1191

FAX Number: (703) 326-4918

From the Washington Beltway (495)

- 1) Exit at the Dulles Toll Road (VA-657) West toward Dulles Airport.
- 2) Exit at the Fairfax County Parkway (VA-7100), turning right
- 3) Immediately get into the left lanes to turn left onto the ramp for Spring Street (the sign indicates Spring Street/Sunset Hills Road).
- 4) Turn right (West) onto Spring Street.
- 5) Continue on Spring Street for approximately 0.6 miles.
- 6) Turn right onto Huntmar Park Drive.
- 7) Turn left into the first parking lot. The SunGard suite is on the first floor of the 3-story office building.

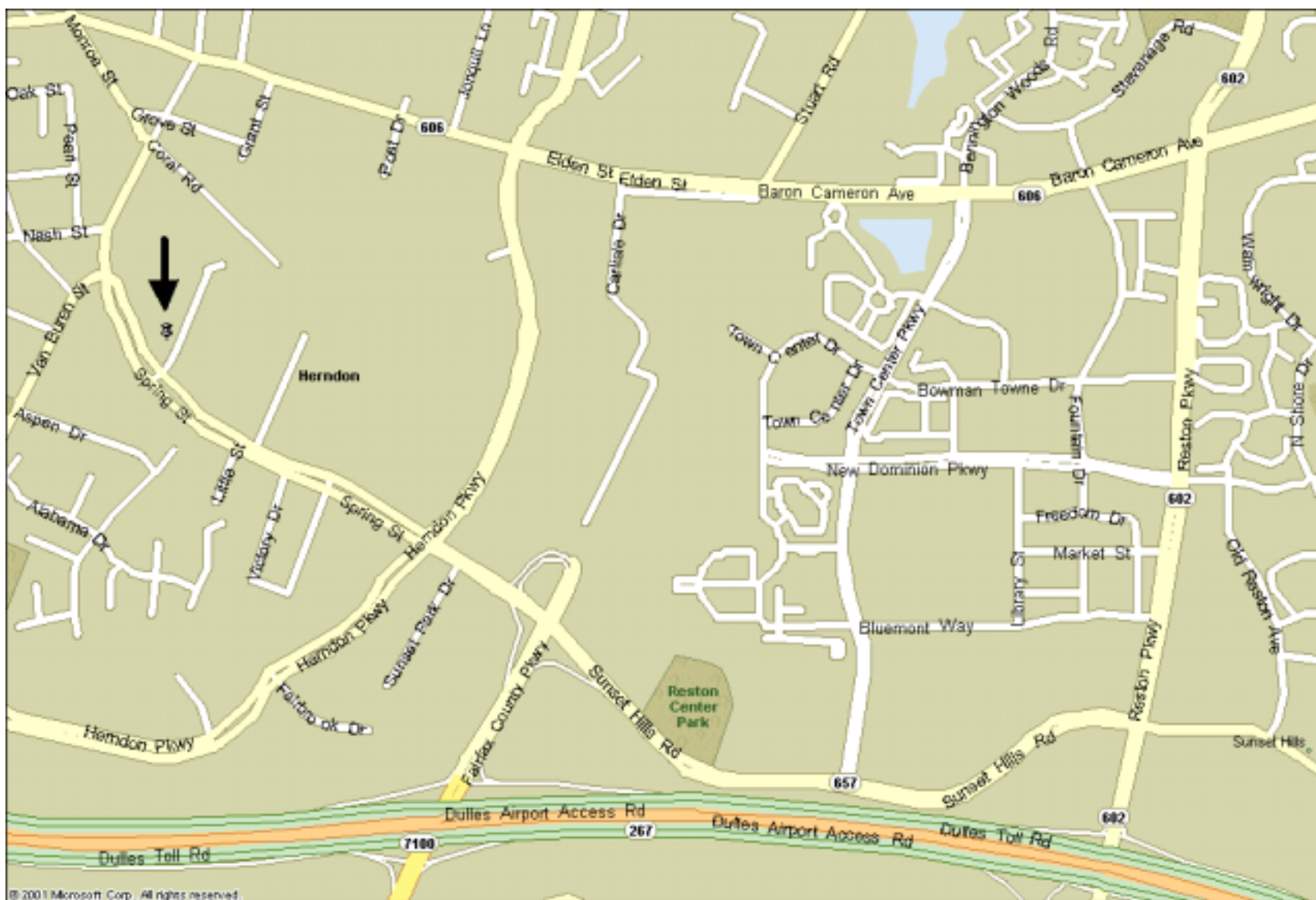
Returning to the Dulles Toll Road

- 1) Turn right out of the parking lot onto Huntmar Park Drive.
- 2) Turn left onto Spring Street.
- 3) Stay in the right lane to the exit ramp to the Fairfax County Parkway.
- 4) Immediately get into the left lanes.
- 5) Cross over the Dulles Toll Road, and turn left to the on-ramp.

Following are: (1) an overview map of the general area around the Herndon facility, (2) a detailed map of the immediate vicinity around the Herndon facility, and (3) alternate routes to the Herndon facility.

Note: The Fairfax County Parkway extends beyond Spring Street, even though the maps do not indicate this.





Alternate Routes to Work Area Recovery Center

Should access via the Washington beltway be impeded, alternate routes to the Dulles Toll Road include:

Via the Theodore Roosevelt Memorial Bridge or the Francis Scott Key Bridge

- 1) Cross the bridges into Virginia and take Interstate 66 West
- 2) Exit at the Dulles Access and Toll Road towards Dulles Airport.

Via the Arlington Memorial Bridge

- 1) Cross Memorial bridge into Virginia and take the George Washington Parkway towards Rosslyn
- 2) Exit at Spout Run (it is a left exit past Key Bridge)
- 3) Turn right at Lee Highway (VA-29)
- 4) Take Interstate 66 West
- 5) Exit at the Dulles Access and Toll Road towards Dulles Airport

Should access via the Dulles Toll Road be impeded, alternate routes include:

Via Virginia Route 7

- 1) From the Washington beltway, exit at VA-7 West (towards Tysons Corner)
- 2) Exit at the Fairfax County Parkway (VA-7100) South

Via Georgetown Pike (VA Route 193)

- 1) From the Washington beltway, exit at Georgetown Pike (VA-193) West
- 2) Turn right onto Leesburg Pike, VA-7
- 3) Take Fairfax County Parkway (VA-7100) South

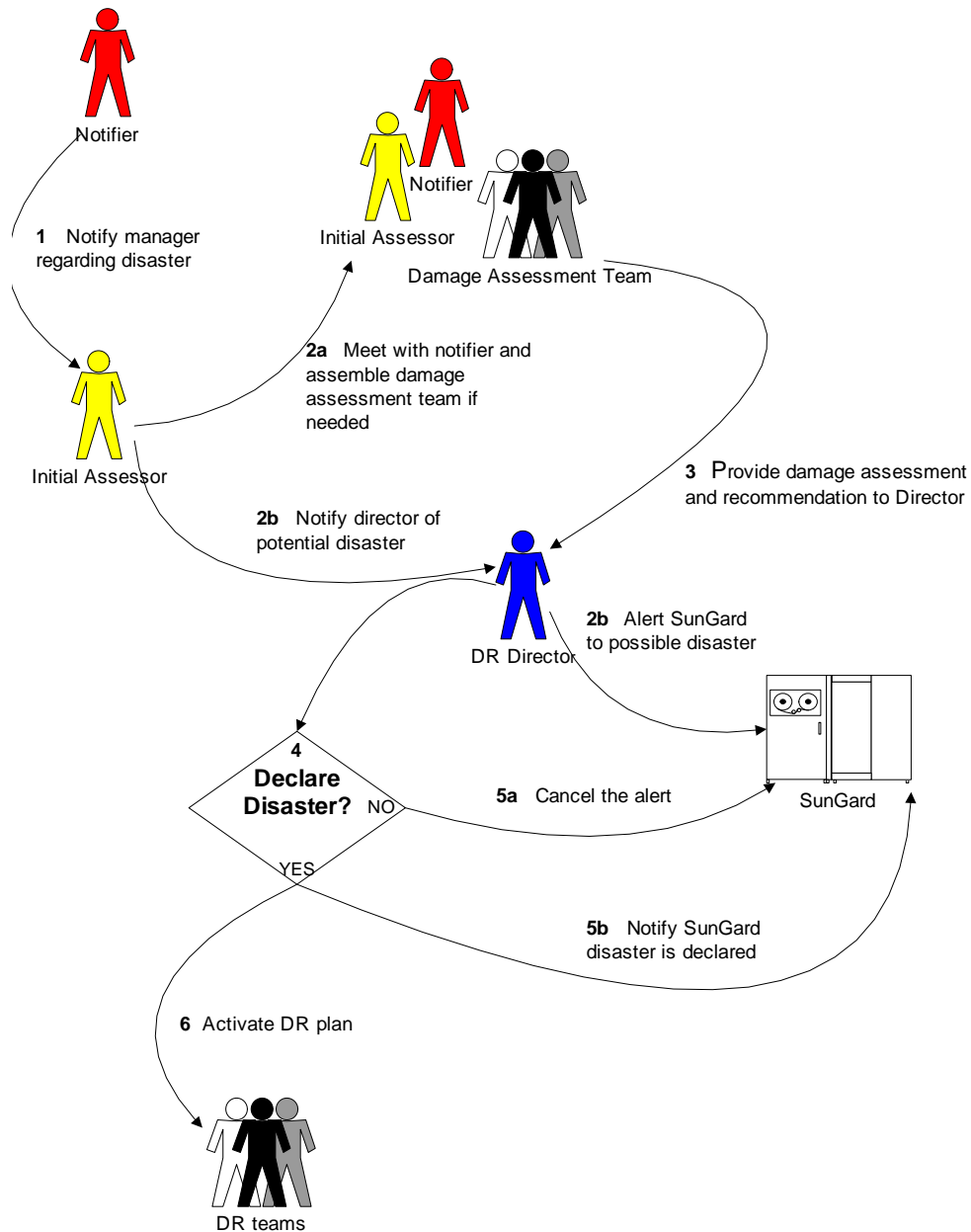
Other alternate route:

From Frederick, MD Via Point of Rocks

From Interstate 70 take US -15 S / US-340 W
Merge onto US-15 S via the exit on the Left towards Leesburg (crossing into Virginia)
Stay straight to go onto US-15 Bypass South / Leesburg Bypass
Exit at VA-657 East, toward Herndon/Chantilly
Exit at the Fairfax County Parkway, turning left

Appendix C – Disaster Alert Procedures, Team Members, and Contact Information

Disaster Alert Process Flow



Disaster Alert Procedures

1) If you are the first person to discover a major problem affecting the Data Center, you become the **notifier**. Do the following:

- Contact the NIH fire and police if you have not already done so and follow evacuation procedures.
- Call the following people in the order listed, until you reach one of them.

Initial Assessor

<i>Contacts:</i>	<i>Home:</i>	<i>Pager/Cell:</i>	<i>Office:</i>
Ed Suiter	301-260-9410	(C)301-646-9327 (P)888-445-0423	301-496-7352
Paul Powell	301-273-3932	(C)240-447-8733	301-594-4945
Adriane Burton	301-564-4240	(C)240-401-5119	301-451-4553
Doug Ashbrook	301-391-6716	(C) 301-830-0837	301-402-1248
Lolly Bennett	301-424-6636	(C)301-830-0851	301-435-5493
Steve Bailey	301-424-2761	(C)301-785-7711	301-435-2981
Kevin Hobson	301-865-4732	(C)301-512-6532 (P)888-452-9534	301-402-4762

Be prepared to tell him or her:

- Your name and phone number where you can be reached.
- What occurred and what parts of the machine room are affected.
- The extent of damages and injuries as far as you can tell.

After passing along that information, you do not need to make any further notifications.

The person responding to the call becomes the **initial assessor** of the disaster. While on the telephone with the notifier, obtain answers to the following:

- Who called you and what is their contact phone number?
- What is the nature of the problem?
- What is the extent of the damage and are there any injuries?
- Can the building be entered?
- Are there any immediate dangers or restrictions?
- Have any other managers been contacted and, if so, who?

You (the **initial assessor**) should tell the notifier:

- when you will arrive and where you will meet him or her, and
- that you will make all further contacts.

2a) The **initial assessor** then goes to NIH Data Center to meet the notifier and to make a preliminary appraisal of the following:

- Whether or not the Data Center can be entered.
- The extent of damage to the building.
- The extent of damage to the computer equipment.

If required, assemble members from the Damage Assessment Team to tour the area and evaluate the extent of the damage. To assemble the team, call the people on the following four lists in the order listed. Once you have reached someone for a platform, go on to the next.

*Mainframe Damage
Assessment*

<i>Contacts:</i>	<i>Home:</i>	<i>Pager/Cell:</i>	<i>Office:</i>
Doug Ashbrook	301-391-6716	(C) 301-830-0837	301-402-1248
John Dussault	202-483-2734	(C)202-460-9002	301-402-1252
Jay Vinton	202-966-0988		301-402-1238

*EOS Damage
Assessment*

<i>Contacts:</i>	<i>Home:</i>	<i>Pager/Cell:</i>	<i>Office:</i>
Lolly Bennett	301-424-6636	(C)301-830-0851	301-435-5493
Jon Burelbach	301-293-1723	(C)240-478-9775	301-496-7372
Paula Moore	301-309-0983	(C)240-478-9772	301-402-1237
Ernie Jordan	301-589-1382	(C)240-328-4177	301-496-6755

*Windows Hosting
Damage Assessment*

<i>Contacts:</i>	<i>Home:</i>	<i>Pager/Cell:</i>	<i>Office:</i>
Howard Bartlow	240-912-7135	(C) 301-830-0846	301-496-5342
Tim Pickett	301-253-4342	(C)240-463-6834	301-435-277
Larry Nice	410-586-1366	(C) 240 478-9773	301-594-9451

*Helix Damage
Assessment*

<i>Contacts:</i>	<i>Home:</i>	<i>Pager/Cell:</i>	<i>Office:</i>
Steve Bailey	301-424-2761	(C)301-785-7711	301-435-2981
Steve Fellini	202-332-8170	(C)202-302-1891	301-496-5182
Mark Patkus	301-949-6966	(P)877-554-5648 (C)301-641-6703	301-402-0370

*Windows I&M
Damage Assessment*

<i>Contacts:</i>	<i>Home:</i>	<i>Pager/Cell:</i>	<i>Office:</i>
7x24 Pager		301-224-4894	
Kevin Hobson	301-865-4732	(C)301-512-6532 (P) 888-452-9534	301-402-4762
Valerie Wampler	410-203-1127	(C)240-401-2752	301-402-7169
Jonathan Thomas	410-360-1008	(C)240-676-2727	301-435-4104

- 2b) The **initial assessor** also notifies Adriane Burton regarding the potential Disaster. Adriane becomes the **DR Director**. If Adriane cannot be reached, the initial assessor becomes the DR Director.

The **DR Director** alerts SunGard to the potential disaster. Reference Appendix D for procedures.

- 3) The **initial assessor, notifier, and Damage Assessment Team** (if assembled) evaluate the damage and the need to activate the disaster recovery plan. Inform the DR Director of the findings and recommendations.
- 4) The **DR Director** makes the decision regarding a disaster declaration.
- 5a) The **DR Director** cancels the alert with SunGard if the problem can be solved within 72 hours. Reference Appendix D for procedures.
- 5b) The **DR Director** notifies SunGard that a disaster is declared if the outage will last longer than 72 hours. Reference Appendix D for procedures.
- 6) The **DR Director** activates the disaster recovery plan.
- a) Establish a disaster recovery command center and convene the Executive Team there. Contact the Executive Team members (who are not already on hand) in the order listed, requesting the first person contacted to notify remaining members.

Executive Team

<i>Members:</i>	<i>Home:</i>	<i>Pager/Cell:</i>	<i>Office:</i>
Adriane Burton	301-564-4240	(C)240-401-5119	301-451-4553
Ed Suiter	301-260-9410	(C)301-646-9327 (P)888-445-0423	301-496-7352
Doug Ashbrook	301-391-6716	(C) 301-830-0837	301-402-1248
Lolly Bennett	301-424-6636	(C)301-830-0851	301-435-5493
Steve Bailey	301-424-2761	(C)301-785-7711	301-435-2981
John Price			
Kevin Hobson	301-865-4732	(C)301-512-6532 (P)301-913-2683	301-402-4762
Adrienne Yang	301-652-7151	(C)301-412-8778	301-496-1053

- b) Notify the key executives regarding the disaster situation. Names and phone numbers are listed under Other Contact Information below.
- c) Establish communications with the Emergency Management Branch in the NIH Division of Public Safety (DPS). They will coordinate the support provided by the teams established by the NIH Continuity of Operations Plan (Public Information, Finance, Logistics, etc.).
- d) Contact operations staff member to pull tapes from the ATL(s) for First Federal pickup and notify First Federal regarding the shipment of the backup tapes to SunGard. Reference Appendix E for procedures.
- e) Contact the disaster recovery team leads or alternate leads (who are not already on hand) to report to the DR command center.
- f) The Disaster Recovery Coordinator works with the team leads/alternate leads regarding reporting instructions for remaining team members.
- g) Contact team members with reporting instructions. Team members and contact information are listed in the next section.
- h) Customer Support Team members notify DR customer contacts. Reference Appendix A for contact information.

Accessibility to the Hot Site Locations

The Restoration Team will report to the work area recovery center in Herndon, VA from which they will manage the restoration of the systems and monitor the systems while in recovery mode operations. A limited number of the Operations team may report to the hot site in Wood Dale, IL to manage the daily operations of the systems.

In the event of an area-wide disaster, available staff will be instructed on where to report after the Executive team has determined when the disaster recovery plan would be activated. Should the Herndon facility be unavailable, selected Restoration Team members will report to Wood Dale, IL and the remaining members will work from home or other NIH facilities. Should Wood Dale be unavailable, SunGard will accommodate NIH at one of their other recovery centers.

Staff will use their private cars to travel to/from the Herndon facility. There are multiple, alternative access routes to Herndon. (Reference Appendix B, Directions to Work Area Recovery Center.) Alternate modes of transportation to the Wood Dale hot site (or other SunGard recovery centers) include commercial airline, train, bus, rental car, and private car.

Disaster Recovery Team Members (and Contact Information)

DISASTER RECOVERY PLANNING AND MANAGEMENT

Disaster Recovery Coordinator: Adrienne Yang

Senior Technical Advisor (Titan): Jay Vinton

Senior Technical Advisor (EOS): Paula Moore

User Support and Liaison (Titan): ????

User Support and Liaison (EOS): Robert Klein

DAMAGE ASSESSMENT TEAM

Lead: Paul Powell

Alternate:

Team Members (Titan): Doug Ashbrook, John Dussault, Jay Vinton

Team Members (EOS): Lolly Bennett, Jon Burelbach, Ernie Jordan, Paula Moore

EXECUTIVE TEAM

Lead: Adriane Burton

Alternate:

Team Members: Doug Ashbrook, Steve Bailey, Lolly Bennett, Kevin Hobson, John Price, Ed Suiter, Adrienne Yang

RESTORATION TEAM (TITAN)

		Home:	Pager/Cell:	Office:
Lead:	Jay Vinton	202-966-0988		301-402-1238
Alternate:	Doug Ashbrook	301-391-6716	(C) 301-830-0837	301-402-1248
Team Members by function:				
Operations & Backup Media:	Paul Powell	301-273-3932	(C)240-447-8733	301-594-4945
	Linwood Genus	301-773-8162	(P)888-982-9792	301-402-3558
	Billy Graham	301-596-4112	(P)888-453-9766	301-402-3541

		<i>Home:</i>	<i>Pager/Cell:</i>	<i>Office:</i>
<i>Tape Management & Recovery:</i>	Humberto Hutchinson	301-249-2023	(P)888-982-9585	301-402-3562
	David O’Brien	919-858-5396	(C)919-818-2353	301-435-5487
	<i>System Software:</i> T.C. Chen	301-963-0326	(C)301-641-5665	301-402-1253
	David Des Roche	301-996-4890	(C)301-996-4890	301-402-1239
	John Dussault	202-483-2734	(C)202-460-9002	301-402-1252
<i>IMS:</i>	Bill Long	301-846-4232	(C)301-830-2650	301-435-5482
	Susie Stout	540-347-0918	(C) 240-205-9475	301-594-7814
	Clyde Colmes	301-601-9416	(C)240-205-5420	301-496-6244
	Pete Nordyke	301-738-9950	(C)240-643-9950	301-402-1246
	<i>Telecommunications:</i> Bobby Bauer	301-649-6262		301-594-7474
	Network Operations Center (NOC)	301-402-3141	(P)301-506-9069	
<i>Data Base:</i>	Angela Bennett	240-683-0958	(P)877-540-2282	301-435-5491
	Hoyte Carelock	301-345-2470	(P)877-320-6936	301-435-5488
	Ed Ryan	202-462-3852	(P)877-554-4956	301-496-1452

RESTORATION TEAM (EOS)

		<i>Home:</i>	<i>Pager/Cell:</i>	<i>Office:</i>	
<i>Lead:</i> <i>Alternate:</i> <i>Team Members by function:</i> <i>Operating System and Restores:</i>		Paula Moore	301-309-0983	(C) 240-478-9772	301-402-1237
		Jon Burelbach	301-293-1723	(C)240-478-9775	301-496-7372
		Ana Arostegui	202-986-6939	(C)240-328-4174	301-451-6071
		Rob Flowers	301-952-8593	(P)888-445-7552 (C) 240-281-8571	301-402-4117
		Karen Johnson	410-486-8113	(C)240-205-9470	301-594-1488
		Diem-An Le	301-515-5821	(C)240-601-5003	301-594-5306
		Mythanh Nguyen	301-725-4154	(C)301-830-0839	301-496-2962
		Tim Salo	301-570-3814	(C)240-205-9472	301-435-4956
		Giao Tran	301-528-8679	(P) 888-445-6936	301-402-3208
<i>Database:</i>		Michelle Ugas	301-384-3835	(C) 301-346-6121	301-325-7674

		<i>Home:</i>	<i>Pager/Cell:</i>	<i>Office:</i>
<i>Firewall:</i>	Sridhar Karegowdra	410-772-1465	(C)443-538-5018	301-496-0894
	Dave Luthra	301-299 2769	(C)301-529 5171	301-435-2740
	Joe Januszewski	410-552-5354	(C)301-830-2642	301-435-5518
	Clint Wimsatt	301-371-9923	(C)301-830-2687	301-435-2084

RESTORATION TEAM (WINDOWS HOSTING)

	<i>Home:</i>	<i>Pager/Cell:</i>	<i>Office:</i>	
<i>Lead:</i>				
<i>Alternate:</i>	Tim Pickett	301-253-4342	(C)240-463-6834	301-435-277
<i>Team Members:</i>	Khoa Le	301-937-4568	(C)301-830-0847	301-496-4049
	Vincent Wong	301-987-0994	(C)240-205-5414	301-435-5495

RESTORATION TEAM (WINDOWS MESSAGING)

		<i>Home:</i>	<i>Pager/Cell:</i>	<i>Office:</i>
<i>Lead:</i>	Jonathan Thomas	410-360-1008	(C)240-676-2727	301-435-4104
<i>Alternate:</i>				
<i>Team Members:</i>	Artie Noel	301-663-6964	(C) 240-478-9766	301-435-2908
	David Shurtliff	703-349-2994	(C) 240-328-5008	301-496-9309

OPERATIONS TEAM

	<i>Home:</i>	<i>Pager/Cell:</i>	<i>Office:</i>
<i>Lead:</i>	Paul Powell	see Restoration Team (Titan) listing	
<i>Alternates/Shift Supervisors:</i>			
<i>Team Members (Titan):</i>	Fritzner Jean	301-384-2170	(P)301-907-2127 301-496-7653
	Linwood Genus	see Restoration Team (Titan) listing	
	Bill Graham	see Restoration Team (Titan) listing	
	Humberto Hutchinson	see Restoration Team (Titan) listing	
<i>IMS:</i>	Clyde Colmes	see Restoration Team (Titan) listing	

	<i>Home:</i>	<i>Pager/Cell:</i>	<i>Office:</i>
Team Members (EOS):	Ernest Jordan	301-589-1382	(C)240-328-4177 301-496-6755

CUSTOMER SUPPORT TEAM

	<i>Home:</i>	<i>Pager/Cell:</i>	<i>Office:</i>
Lead:	see Executive Team (step 6a) listing		
Alternate:	Jim Gangler	301-299-2331	301-496-7337
Team Members (Titan):			
Team Members (EOS):	Robert Klein	301-649-2221	301-496-7400

SALVAGE RECLAMATION TEAM

	<i>Home:</i>	<i>Pager/Cell:</i>	<i>Office:</i>
Lead:	Adriane Burton	see Executive Team (step 6a) listing	
Alternates:	Ed Suiter	see Executive Team (step 6a) listing	
	Paul Powell	see Restoration Team (Titan) listing	
Team Members:			
	Joe Hoffman	(C)443-226-7300	301-496-6665
	Andrew Prandoni	301-762-1725 (P)888-982-5313	301-435-5293

ADMINISTRATIVE SUPPORT TEAM

	<i>Home:</i>	<i>Pager/Cell:</i>	<i>Office:</i>
Lead:			
Alternate:	Adriane Burton	see Executive Team (step 6a) listing	
Team Members:	Rhonda Harrison	301-899-3820	301-496-0388

Other Contact Information**Key Executives Contact Information (contact in the order listed)**

	<i>Office</i>	<i>Contact</i>
Jack Jones Acting, Chief Information Officer, CIT	301-496-5703	(H)703-556-6513 (C)301-728-3331
Al Whitley Deputy Director, CIT	301-496-5704	
Kathy Wimsatt Executive Officer, CIT	301-496-0513	(H)301-977-3314 (C)301-748-1081
Renita Anderson, Director, DNST, CIT	301-594-9432	(H)301-249-9785 (C)301-529-1985
Chris Ohlandt, Director, DCS	301-496-6877	
Jack Vinner Acting Director, DECA	301-435-5292	

Key Contact Information

<i>Agency/Service</i>	<i>Contact</i>
NIH Fire/Rescue	911 (Emergency) 301-496-5685 (Non-Emergency)
NIH Police	911 (Emergency) 301-496-5685 (Non-Emergency)
DPS, Emergency Management Branch	301-496-1985
Dawn Farr, ISSO	301-402-4449 (O) 301-407-2279 (H) 301-367-1443 (cell)
CDC Operations Help Desk	404-639-7810 404-639-7500
FMS (US Treasury) Network Group Help Desk	202-874-8725 202-874-4357
SSA Control Center Help Desk	410-966-5463 410-965-7777
USBank of Minnesota Help Desk	800-765-9549

Appendix D – Hot Site Contact Information and Emergency Procedures

Contact Information

The DCSS hot site contract is with SunGard Availability Services. The following are key SunGard contacts associated with the NIH Data Center's Disaster Recovery Program:

Kathleen Hamilton, Account Executive, Public Sector
SunGard Availability Services
505 Huntmar Park Drive
Herndon, VA 20170
(office) 703-326-4923 (cell) 443-268-4672
Kathleen.hamilton@sungard.com

Yolanda Rivera, Customer Care Specialist II
SunGard Availability Services
711 North Edgewood
Wood Dale, IL 60191
(office) 630-616-5124 (fax) 312-408-1489
yolanda.rivera@sungard.com

Test Scheduling
1-800-541-8378

The following DCSS managers are authorized to notify SunGard regarding an alert or disaster:

Adriane Burton
Ed Suiter
Paul Powell
Doug Ashbrook
Lolly Bennett
Steve Bailey
Kevin Hobson

Emergency Procedures

SunGard requests subscribers to place SunGard on “Alert” notice in the event of a pending disaster to determine if or monitor when a disaster should be declared.

Use the following procedures for disaster alerts and disaster declarations:

- 1) Call the 24-hour Disaster and Alert Notification Hotline at 1-866-722-1313.
- 2) Be prepared to provide the following information:

Type of notification:	<i>Alert or Disaster</i>
Organization name:	<i>National Institutes of Health</i>
City and State:	<i>Bethesda, MD</i>
Caller’s Identification:	Your name and phone number, plus alternate phone numbers such as cell phone number, pager number, and/or home phone number
Location of the incident or disaster	
Nature of the incident or disaster	
Hardware affected	
SunGard Facility Subscription:	<i>Wood Dale, IL (host systems) and Herndon, VA (work group)</i>
Identifier:	<i>09-RS2585</i>
Estimated time of arrival (for disaster only)	

A form for recording pertinent information before making the call is provided at the end of these instructions.

- 3) Someone from the SunGard Crisis Management Team will contact you to confirm the Alert/Disaster.
- 4) If the call is an **alert notification**, the Crisis Management Team and/or the NIH Account Executive or Customer Service Coordinator will check in with you at prearranged intervals to stay abreast of the situation until the event is resolved by either termination of the alert or a resulting disaster notification.
- 5) If the call is a **disaster notification**:
 - a) Upon authorization of the disaster, the Crisis Management Team will invoke operations at the SunGard centers affected.
 - b) The Crisis Management Team, Operations and Customer Service will review with us our last test plans to identify the accuracy, resources, supplies and services needed for the recovery. Our recovery configuration will also be reviewed to identify any

additional provisions we may require. The recovery configuration is created at time of disaster.

- c) Upon our arrival at the SunGard recovery centers, we will be acquainted with our areas of operations and appropriate procedures.
- d) SunGard will assist with setting up command or control centers if required.
- e) NIH must provide SunGard a written letter (on letterhead) within 24 hours stating we have declared a disaster and including the following information: platforms affected, date and time of the declaration, and the reason the disaster was declared. A fax is acceptable.
- f) NIH must provide SunGard written notification of disaster completion.

Disaster/Alert Notification Form

Disaster Notification: ☐ Yes ☐ No

Alert Notification: ☐ Yes ☐ No

Organization Name: National Institutes of Health

City & State: Bethesda, MD

Caller's Name: _____ **Caller's Phone Number:** _____

Alternate Phone Number:

Cell#: _____ **Beeper#:** _____ **Home#:** _____

Location of Incident or Disaster: _____

Nature of Incident or Disaster: _____

Hardware Affected: _____

SunGard Facilities: Wood Dale, IL (host systems) and Herndon, VA (work group)

Identifier: 09-RS2585

FOR DISASTER ONLY

Estimated Time of Arrival: _____

Appendix E - Off-Site Storage Information and Emergency Procedures

First Federal Storage Facility

The DCSS off-site storage contract is with the First Federal Corporation located at 75 West Watkins Mill Road, Gaithersburg, MD 20878, approximately 13 miles from the NIH Data Center. This site is sufficiently separated from the Data Center to ensure that explosions, fire and water damage affecting the Data Center facility will not affect the off-site storage facility. Power outages may or may not affect both facilities depending on how wide spread the outage. Both facilities have uninterruptible power supplies to provide electrical power to their facilities during power outages.

General Contact Information

The main phone numbers are: 301-548-1500 (Administration)
1-888-735-3500

Operations Department: Phone: 301-548-9676
Administration FAX: 301-548-0682
Operations FAX: 301-963-8974

Authorized DCSS Employees

Only designated employees who have been issued First Federal ID badges may request tape deliveries and/or manage the backup tape storage procedures, per their authorization codes.

NAME:	CODE # 1 2 3 4 5 6 7 8 9
Berluche, Marie	7 8 9
Cleaveland, Jeannie	7 8 9
Genus, Linwood	7 8 9
Graham, Billy	1 2 3 4 5 6 7 8 9
Henderson, Jennifer	7 8 9
Horner, Richard W.	7 8 9
Jean, Fitzner	7 8 9
Jones, Glenn	7 8 9
Jordon, Ernerst T.	1 2 3 4 5 6 7 8 9
Nguyen, Hiep	7 8 9
Palmaila, Ramil	7 8 9
Powell, Paul A.	1 2 3 4 5 6 7 8 9
Proctor, Benita	7 8 9
Small, Jane	1 2 3 4 5 6 7 8 9
Suiter, Ed	1 2 3 4 5 6 7 8 9
Yang, Adrienne	3 6

- Code # 1: Authorized to add, delete and change names of authorized personnel, and perform functions 2 through 9 inclusive.
- Code # 2: Authorized to make temporary changes to delivery schedules, including cancellation or rescheduling of regular delivery services.
- Code # 3: Authorized to access First Federal facilities for inventory and inspection purposes.
- Code # 4: Reserved for future use.
- Code # 5: Authorized to deliver, release and/or retrieve media at First Federal (during regular business hours).
- Code # 6: Authorized to invoke formal disaster recovery procedures.
- Code # 7: Authorized to call for and receive regularly scheduled delivery services.
- Code # 8: Authorized to call for and receive regular and non-scheduled (within 24 hours) delivery service, during normal working hours.
- Code # 9: Authorized to call for and receive regular, non-scheduled and emergency delivery service, 24 hours per day, 365 days per year.

Emergency Procedures

- 1) Call First Federal at 301-548-9676 or 1-888-735-3500.
- 2) Be prepared to provide the following information:
 - your full name and First Federal ID badge number,
 - the company name (*NIH Computer Center*),
 - the telephone number from which you are calling, and
 - the total number of media to be delivered.
- 3) If calling after normal business hours (which are Monday through Friday, 9:00 am to 5:00 pm), specify that an After Hours Emergency Delivery within two hours is required.

A First Federal employee assigned to the after hours duties will promptly return your call and request verification of the information supplied above. Upon determination that the request for Emergency Service is valid, the delivery will proceed.

Note: The employee actually receiving the media must be in possession of a valid First Federal ID badge, issued at Code #6 or #9 when the delivery is made.

First Federal personnel must satisfactorily confirm that the request for emergency delivery is legitimate. In the event that an emergency delivery is declined for security reasons, First Federal will make every reasonable effort to notify a senior employee on the Authorization List of an apparently unauthorized request for service.

Directions to the First Federal Gaithersburg Facility

Via Interstate 270 North from the Washington Beltway toward Frederick, MD

- 1) Proceed North to Exit 10 - Clopper Road, Route 117.
- 2) Follow Clopper Road approximately 1 mile, cross over Quince Orchard Road.
- 3) Turn right on West Watkins Mill Road.
- 4) Proceed to the end of the road and turn left.
- 5) Continue straight ahead to #75 on the right.

Via Interstate 270 South from Frederick MD toward Washington DC

- 1) Proceed south to Exit 11 - Quince Orchard Road.
- 2) Follow Quince Orchard Road for approximately 1 mile.
- 3) Turn Right onto Clopper Road.
- 4) Turn right on West Watkins Mill Road
- 5) Proceed to the end of the road and turn left.
- 6) Continue straight ahead to #75 on the right.

Off-Site Automated Tape Library

The off-site tape library is located in the NIH Consolidated Co-Location Site (NCCS), which is housed in a secure, environmentally controlled vendor facility (Qwest Communication Corporation) located at 22830 International Drive, Sterling, VA 20166.

Telephone number: 1-800-884-3082

Emergency Information

Selected DCSS staff have been granted unlimited access to the Qwest facility either by being issued a Qwest ID badge (badge access) or being pre-registered with Qwest for frequent visits (non-badge access requiring escort). These individuals would have access to the NCCS in case of a disaster event in the Data Center.

DCSS staff registered with Qwest are:

Name	DCSS Branch	Access Hours	Access Level
Akeem, Carleen	ASB	24x7	Badge
Arostegui, Ana	HSB/Unix	24x7	Badge
Bennett, Laura	HSB	24x7	Badge
Boswell, Steven	HSB/Win Hosting	24x7	Badge
Burelbach, Jonathan	HSB/Unix	24x7	Badge
Dildine, Scott	EMIB	24x7	Badge
Floura, Ranvir	HSB/Firewall	24x7	Badge
Flowers, Robert	HSB/Unix	24x7	Badge
Januszkeski, Joseph	HSB/Firewall	24x7	Badge
Jean, Fritzner	DCOB	24x7	Badge
Jordan, Ernest	DCOB	24x7	Badge
Le, Khoa	HSB/Win Hosting	24x7	Badge
Malloy, Tim	EMIB	24x7	Badge
Moore, Paula	HSB/Unix	24x7	Badge
Nguyen, Mythanh	HSB/Unix	24x7	Non-Badge
Nice, Larry	HSB/Win Hosting	24x7	Badge
Palmaira, Ramil	DCOB	24x7	Badge
Powell, Paul	DCOB	24x7	Badge
Scalzi, Kathy	ASB	24x7	Non-Badge
Shurtliff, David	EMIB	24x7	Badge
Stout, Susie	LSSB	24x7	Badge
Suiter, Ed	DCOB	24x7	Badge
Tran, Quynh-Giao	HSB/Unix	24x7	Badge
Wimsatt, Clinton	HSB/Firewall	24x7	Badge
Wong, Vincent	HSB/Win Hosting	24x7	Badge

Directions to the Qwest Facility

Via the Washington Beltway (495)

- 1) Exit at the Dulles Toll Road (VA-657) West toward Dulles Airport.
- 2) Exit at Route 28 North.
- 3) Follow Route 28 North through the first traffic light.
- 4) Get in the right lane and take next exit to Route 606 - Old Ox Road/Shaw Road, following the Shaw Road direction (which will be a slight left as you exit from Route 28). You will come to a stop light.
- 5) Proceed through the traffic light and immediately get into the left-most lane.
- 6) Turn left onto Shaw Road at the first traffic light.
- 7) Proceed ¼ mile and turn left onto International Drive.
- 8) Turn left into the second parking lot and proceed to the middle building. (You will see a NO Trespassing sign.)
- 9) The facility is unmarked except for the building number, 22860, above the door.

Alternate Routes to the Off-Site Storage Facilities

First Federal

Should access via Interstate 270 be impeded, alternate routes to the facility include:

Via Maryland Route 355 North from Bethesda

- 1) Proceed North to Clopper Road, Route 117.
- 2) Turn left on Clopper Road, crossing over Quince Orchard Road.
- 3) Turn right on West Watkins Mill Road.
- 4) Proceed to the end of the road and turn left.
- 5) Continue straight ahead to #75 on the right.

Via Maryland Route 355 South from Frederick

- 1) Proceed south to Clopper Road, Route 117.
- 2) Turn Right onto Clopper Road, crossing over Quince Orchard Road.
- 3) Turn right on West Watkins Mill Road
- 4) Proceed to the end of the road and turn left.
- 5) Continue straight ahead to #75 on the right.

Alternate Routes to the Qwest Facility

Should access via the Washington beltway be impeded, alternate routes to the Dulles Toll Road include:

Via the Theodore Roosevelt Memorial Bridge or the Francis Scott Key Bridge

- 1) Cross the bridges into Virginia and take Interstate 66 West
- 2) Exit at the Dulles Access and Toll Road towards Dulles Airport.

Via the Arlington Memorial Bridge

- 1) Cross Memorial bridge into Virginia and take the George Washington Parkway towards Rosslyn
- 2) Exit at Spout Run (it is a left exit past Key Bridge)
- 3) Turn right at Lee Highway (VA-29)
- 4) Take Interstate 66 West
- 5) Exit at the Dulles Access and Toll Road towards Dulles Airport

Should access via the Dulles Toll Road be impeded, alternate routes include:

Via Virginia Route 7

- 1) From the Washington beltway, exit at VA-7 West (towards Tysons Corner)
- 2) Turn left onto North Sterling Boulevard which turns into South Sterling Boulevard
- 3) Turn left onto Shaw Road
- 4) Turn right onto International Drive

Via Georgetown Pike (VA Route 193)

- 1) From the Washington beltway, exit at Georgetown Pike (VA-193) West
- 2) Turn right onto Leesburg Pike, VA-7
- 3) Turn left onto Shaw Road
- 4) Turn right onto International Drive

Other alternate route:

From Frederick, MD Via Point of Rocks

- 1) From Interstate 70 take US -15 S / US-340 W
- 2) Merge onto US-15 S via the exit on the Left towards Leesburg (crossing into Virginia)
- 3) Stay straight to go onto US-15 Bypass South / Leesburg Bypass
- 4) Exit at VA-7 East ramp
- 5) Turn slight right onto VA-7 East/East Market Street and continue to follow VA-7 East.
- 6) Merge onto VA-28 South/Sully Road towards Dulles Airport/Centreville.
- 7) Merge onto South Sterling Boulevard/VA-846 North.
- 8) Turn Right onto Shaw Road.
- 9) Turn Right onto International Drive.

Appendix F1 – Titan Restore Procedures

General Information

Reading an Internally Labeled Tape

If you need to read an internally labeled tape before proceeding, the dataset \$CDS1.MISC.CNTL on the SunGard floor system has a member, TAPELABEL, which uses IEBGENER to copy the labels from a tape to sysout using BLP (Bypass Label Processing).

Using Visara to Access SunGard DR System Console or TSO

Any PC having a tn3270 application such as QWS can be used to access the SunGard disaster recovery LPARs during a disaster recovery test or an actual disaster.

The following procedure to set up the session applies when the LPAR is running the SunGard floor system, NIH DR System 4, or NIH DR System 9.

Set up a tn3270 session as follows:

```
Hostname = drvisara.cit.nih.gov
Terminal type = IBM-3278-2
Port = 23
Lu name = sunXcon or sunXalt (or sunX for a TSO session)
"Enable Security Connection" must be unchecked
```

Where X is the number of the desired SunGard LPAR.

Note: Normally, this will only work from inside NIHnet (including VPN connections to NIHnet).

Scratch Tapes

The scratch tapes are 040800 through 040999.

Information About Backups

All disks except for those used by DB2 are backed up by the Storage Administrators. After all of the backup jobs have completed, a list indicating the disk volser, the data set name on tape, the data set sequence number, and the tape volser is produced. This list is written to tape E00001 with the data set name NIH.STGADMIN.DRMAIL and is also emailed to the Public Distribution List CIT DCSS DRlistings. Similar information for the DB2 backup tapes is written to tape E00002 with the data set name ZDB2DB2.DB2.DISKSAVE.DRTAPE. Each tape has information for each dump cycle with the most recent cycle appearing first.

If a copy of the appropriate email is not available at the disaster site, you can print the list with the following JCL:

```
//JDALIST JOB (),'LIST DISASTER TAPES',
//          MSGCLASS=H,NOTIFY=$JDA
//* LIST FIRST DATA SET ON TAPES E00001 AND E00002
//*
//STEP1 EXEC PGM=IEBGENER
//SYSUT1 DD DSN=NIH.STGADMIN.DRMAIL,
//          LABEL=(1,SL),
//          UNIT=R9840,
//          VOL=SER=E00001,
//          DISP=(OLD,KEEP)
//SYSUT2 DD SYSOUT=*
//SYSPRINT DD SYSOUT=*
//SYSIN DD DUMMY
//*
//STEP2 EXEC PGM=IEBGENER
//SYSUT1 DD DSN=ZDB2DB2.DB2.DISKSAVE.DRTAPE,
//          LABEL=(1,SL),
//          UNIT=R9840,
//          VOL=SER=E00002,
//          DISP=(OLD,KEEP)
//SYSUT2 DD SYSOUT=*
//SYSPRINT DD SYSOUT=*
//SYSIN DD DUMMY
```

In the event of an actual disaster, we would eject tapes E00001 and E00002 and send them to the disaster site with the other tapes. However, if we were to do this for a test, then the weekend jobs attempting to write the new dump information to these tapes would fail because the tapes are not in our silo. To avoid this situation, we have assigned tapes DR0001 and DR0002 with retention periods of 9999 days (which is the maximum value allowed). After the dumps have been created for a particular disaster test, the Storage Administrators should copy tape E00001 to DR0001 and tape E00002 to DR0002. Tapes DR0001 and DR0002 should then be ejected and sent to the disaster site with the other tapes. The JCL that can be used to create these copies is found in NIH.STGADMIN.DIST.WORK.CNTL(COPYTAPE):

```
//JDACOPY JOB (),'COPY DR TAPES',MSGCLASS=H,NOTIFY=$JDA
//*
//*****
//* JOB TO COPY TAPES WITH DUMP INFORMATION (E00001 AND E00002) TO *
//* TAPES (E00101 AND E00102) THAT CAN THEN BE EJECTED FOR A DISASTER *
//* RECOVERY TEST *
//*****
//*
//COPY1 EXEC PGM=IEBGENER
//SYSPRINT DD SYSOUT=*
//*
//SYSUT1 DD DSN=NIH.STGADMIN.DRMAIL,DISP=SHR
//*
//SYSUT2 DD DSN=NIH.STGADMIN.DRMCOPY,
//          UNIT=R9840,
//          LABEL=(1,SL),RETPD=9999,
//          VOL=SER=(E00101),
```

```
//    DISP=(OLD,KEEP)
// *
//SYSIN    DD DUMMY
// *
//COPY2    EXEC PGM=IEBGENER
//SYSPRINT DD SYSOUT=*
// *
//SYSUT1   DD DSN=ZDB2DB2.DB2.DISKSAVE.DRTAPE,DISP=SHR
// *
//SYSUT2   DD DSN=ZDB2DB2.DB2.DISKSAVE.DRCOPY,
//    UNIT=R9840,
//    LABEL=(1,SL),RETPD=9999,
//    VOL=SER=(E00102),
//    DISP=(OLD,KEEP)
// *
//SYSIN    DD DUMMY
```

Note that the data set names on tapes E00101 and E00102 is slightly different (NIH.STGADMIN.DRMCOPY and ZDB2DB2.DB2.DISKSAVE.DRCOPY) than those on tapes E00001 and E00002. Consequently, if you need to list the data from either tape, adjust your JCL accordingly.

The data sets on all four tapes (E00001, E00002, DR0001, and DR0002) are cataloged.

Load FDRABR Software

FDRABR (Fast Dump Restore/Automatic Backup and Restore) is used to back up and restore Titan volumes for disaster recovery purposes. FDRABR is not installed on the hot site system; FDRABR must be installed before proceeding with restoring the Titan volumes.

Several useful listings are created with every set of Titan backups:

- DRLIST1 and DRLIST2 – lists the dumps by volume name with the tape data set name and the tape volume containing the backup. These lists are automatically emailed to all members of the CITDCSSDRLISTINGS and CITDCSSAUTO groups each Saturday after backups have completed.
 - STGSVOLS or STGDVOLS – lists the contents of each backup tape.
 - STGEJECT – lists the backup tapes required to restore the system at the hot site. This list is also emailed to all members of the CITDCSSDRLISTINGS and CITDCSSAUTO groups.
 - STGATLST – lists all tapes in the offsite ATL.
- 1) Determine which LPAR is assigned to System 4 from the SunGard-supplied Web-based mainframe test plan in the table under the heading, LPAR Setup. Confirm the SunGard floor system is up and available to us.

- 2) Logon to the floor system with the user ID **SG01** (logon range is SG01 through SG20).
- 3) **Copy the FDRABR software from tape to disk using the 9840 tape drives in Wood Dale.**
 Create the JCL to do this by modifying one of the existing IEBCOPY jobs contained in SRS.JCL.CNTL (on the SunGard floor system) to match the following JCL:

```

..... //SG01A JOB 'IEBCOPY-3490-TAPE',CLASS=A,
..... //  TIME=10,NOTIFY=SG01,MSGCLASS=D
..... //COPY1 EXEC PGM=IEBCOPY,REGION=0K
..... //SYSPRINT DD SYSOUT=*
..... //IN1 DD DSN=NIH.STGADMIN.DISTBKUP.STARTUP.GXXXXV00,
..... //  VOL=SER=E00XXX,LABEL=(3,SL),
..... //  UNIT=CART9840,DISP=(OLD,KEEP,KEEP)
..... //OUT1 DD DSN=SG01.STARTUP.CNTL,
..... //  UNIT=3390,VOL=SER=2A0CAT,
..... //  DISP=(NEW,CATLG,DELETE),SPACE=(TRK,(25,1,10),
..... //  DCB=(RECFM=FB,LRECL=80,BLKSIZE=6160,DSORG=PO)
..... //SYSUT3 DD UNIT=SYSDA,SPACE=(CYL,(5,1),RLSE)
..... //SYSUT4 DD UNIT=SYSDA,SPACE=(CYL,(5,1),RLSE)
..... //SYSIN DD *
..... COPY OUTDD=OUT1,INDD=IN1
..... /*
..... //

```

where Gxxxxv00 is the most current startup volume (see STGSVOLS or STGDVOLS output),

E00xxx is the tape volume (see DRLIST1 output),

STGADMIN4 output is available in NIH.STGADMIN.PROD.JCL

Note: Check either STGSVOLS or STGDVOLS in the SHOWVOL section near the end of the listing. Look for NIH.STGADMIN.DISTBKUP.STARTUP(0). The GDG name will be shown along with the 9840 tape volume, file sequence number, and creation date.

Save the JCL, and submit the job, noting the time and job number. Verify the job completes successfully (Condition Code 0000).

Job Number _____, Time Submitted _____, Cond Codes _____

This IEBCOPY job creates the SG01.STARTUP.CNTL partitioned data set on VOL=SER=2A0CAT containing the following members:

#README	Information
ABRSTART	loads the FDR/ABR libraries at SunGard
	closes the FDRABR (openexit) at SunGard
	imports and assigns alias name (FDRABR.#) at SunGard
DRPEXTRA	FDR (DRP) parm member extra for adhoc volumes
DRPJCL1	FDR (DRP) production JCL for FDRDRP restores
DRPPARM1	FDR (DRP) parm for system volumes
DRPPARM2	FDR (DRP) parm for Titan LIB volumes

DRPPARM3	FDR(DRP) parm for Titan database volumes
DRPPARM4	FDR(DRP) parm for additional Titan volumes
EXTRAIEB	Extra single IEBCOPY JCL
INIQUECK	used to initialize volumes
INTVVDS	used to initialize VVDs on volumes
OLDIDCAM	old JCL (import ABR catalog to SunGard catalog)
OLDZAPOP	old JCL (disable ABR open exit routine)
RESTORE1	restores ABRSYS and TMS001 volumes (control dataset, ABR catalog, and tape management data sets required by FDRABR).
SCRSM1	old JCL (restores the SCRSM1 volume)
SUNCICS	used to load CICS volumes
END	

- 1) **Load the FDRABR software using the SunGard floor system.** Edit the **ABRSTART** member by replacing the dot (.) placeholders (in bold and underlined) with the appropriate digits, save the changes, and submit the job, noting the time and job number.

```
//SG01A JOB ( ), 'FDR-LIBRARY', CLASS=A, TIME=15,
// MSGCLASS=D, NOTIFY=SG01
//*****
//* JCL FOR USE FOR DISASTER RECOVERY - ALL STEPS MUST COMPLETE *
//* ASSUMPTIONS: GENERIC FOR 9840 CARTRIDGE = CART9840 *
//* SYS MASTER CATALOG VOLID IS 2A0CAT *
//* STEP1 RESTORES FDRABR SOFTWARE TO DR DASD *
//* COPY INDD=((IN1,R)), OUTDD=OUT1 TO REPLACE MEMBERS *
//* COPY INDD=IN1, OUTDD=OUT1 *
//* STEP2 DISABLES FDRABR OPENEXIT ROUTINE *
//* STEP3 IMPORTS THE ABR USERCAT TO DR MASTERCAT (CATALOG.V2A0CAT) *
//* STEP4 CONNECTS ALIASES REQUIRED FOR DR *
//*****
//* STEP 1: CHANGE IN1 GENERATION (####) AND INPUT TAPE (TTTTTT) *
//*****
//STEP1 EXEC PGM=IEBCOPY, REGION=0K
//SYSPRINT DD SYSOUT=*
//IN1 DD DSN=PCC.OFFSITE.FDRLIB2.G0...V00,
// UNIT=CART9840, VOL=SER=E00...,
// LABEL=(1,SL), DISP=(OLD,KEEP,KEEP)
//OUT1 DD DSN=SUN1.FDRABR.LOADLIB, UNIT=3390, VOL=SER=2A0CAT,
// SPACE=(TRK,(425,15,50)), DISP=SHR
//SYSUT3 DD UNIT=SYSDA, SPACE=(TRK,(3,3))
//SYSUT4 DD UNIT=SYSDA, SPACE=(TRK,(3,3))
//SYSIN DD *
COPY INDD=((IN1,R)), OUTDD=OUT1
/*
//STEP2 EXEC PGM=FDRZAPOP, REGION=6144K
//STEPLIB DD DSN=SUN1.FDRABR.LOADLIB, UNIT=3390, VOL=SER=2A0CAT, DISP=SHR
//SYSPRINT DD SYSOUT=*
//SYSLIB DD DSN=SUN1.FDRABR.LOADLIB, UNIT=3390, VOL=SER=2A0CAT, DISP=SHR
//SYSIN DD *
ZAP DISABLE=OPENEXIT
/*
//STEP3 EXEC PGM=IDCAMS, REGION=0K
//SYSPRINT DD SYSOUT=*
```

```
//SYSIN DD *
IMPORT CONNECT -
  OBJECTS( -
    (VSAM.VPCCX.CATALOG.ABRBASE -
    VOLUME(ABRSYS) -
    DEVICETYPE(3390))) -
  CATALOG(CATALOG.V2A0CAT)
/*
//STEP4 EXEC PGM=IDCAMS,REGION=0K
//SYSPRINT DD SYSOUT=*
//SYSIN DD *
  DEFINE ALIAS (NAME(FDRABR) RELATE(VSAM.VPCCX.CATALOG.ABRBASE))
  DEFINE ALIAS (NAME(#) RELATE(VSAM.VPCCX.CATALOG.ABRBASE))
/*
//
```

Job Number _____, Time Submitted _____, Cond-Codes _____

Note: Step 1 information can be found in DRLIST1.

When this job is completed, the FDRABR software has been loaded, the open exit for FDR has been turned off, and the aliases (FDRABR and #) have been imported and attached to the SunGard catalog. Now ready to start loading the two volumes needed by FDRABR(DRP) disaster software

- 2) **Load the two (2) critical volumes needed by FDRABR.** Edit the **RESTORE1** member to restore ABRSYS and TMS001. **JCL changes are necessary by replacing the dot (.) placeholders (in bold and underlined) with the appropriate digits.** See the comments at the beginning of the JCL regarding the changes.

Use DRLIST2 to find the following information for ABRSYS and TMS001:

- Dataset names
- Tape label information
- Volume serial number of the 9840 backup tape

```
//SG01ABR JOB (),'CRITICAL-RESTORES',CLASS=A,TIME=60,
// NOTIFY=SG01,MSGCLASS=D
//*****
/* DR JCL TO RESTORE THE FIRST TWO CRITICAL VOLUMES: *
/* ABRSYS (ABR CATALOGS) AND TMS001 (TMS CATALOGS) *
/* ASSUMES: MCAT IS 2A0CAT; 9840 GENERIC DEVICE IS CART9840 *
/* CHANGES REQUIRED (SEE DRLIST1 AND DRLIST2 OR TAPE E00001): *
/* VERIFY CATALOG NAME=2A0CAT *
/* CHANGE 'DISK1' TO TARGET DASD ADDRESS *
/* CHANGE 'TAPE1' TO BACKUP (SOURCE) TAPE VOLUME NUMBER *
//*****
//ABRSYS EXEC PGM=FDRABR,REGION=4M
//STEPLIB DD DSN=SUN1.FDRABR.LOADLIB,UNIT=3390,VOL=SER=2A0CAT,DISP=SHR
//SYSPRINT DD SYSOUT=*
//SYSPRIN1 DD SYSOUT=*
//DISK1 DD UNIT=3390,VOL=SER=SG....,DISP=OLD
```

```
//TAPE1 DD DSN=FDRABR.VABRSYS.C20...00,
// UNIT=CART9840,VOL=SER=E00...,
// LABEL=(1,SL),DISP=(OLD,KEEP,KEEP)
//SYSIN DD *
RESTORE TYPE=FDR,CONFMESS=NO,CPYVOLID=YES,VOLRESET=YES
SELECT VOL=ABRSYS,NVOL=SG...,TAPEDD=1
/*
//TMS001 EXEC PGM=FDRABR,REGION=4M
//STEPLIB DD DSN=SUN1.FDRABR.LOADLIB,UNIT=3390,VOL=SER=2A0CAT,DISP=SHR
//SYSPRINT DD SYSOUT=*
//SYSPRIN1 DD SYSOUT=*
//DISK1 DD UNIT=3390,VOL=SER=SG...,DISP=OLD
//TAPE1 DD DSN=FDRABR.VTMS001.C20...00,
// UNIT=CART9840,VOL=SER=E00...,
// LABEL=(2,SL),DISP=(OLD,KEEP,KEEP)
//SYSIN DD *
RESTORE TYPE=FDR,CONFMESS=NO,CPYVOLID=YES,VOLRESET=YES
SELECT VOL=TMS001,NVOL=SG70A1,TAPEDD=1
/*
//
//
//* .....IF VOLUME IS (SMS) VOLUME USE BELOW CONTROL STATEMENT.....
RESTORE TYPE=FDR,CONFMESS=NO,CPYVOLID=YES,VOLRESET=YES,SMSPROT=NONE
```

Submit the job.

Job Number _____, Time Submitted _____, Cond-Codes _____

Verify the job completes successfully (Cond-Code 0000). The ABRSYS and TMS001 volumes are now loaded.

When all preceding steps have successfully completed, the volumes needed to IPL the system can be loaded. Fix any failures or start over.

Restore System Volumes

The JCL for restoring the system volumes has been loaded with the FDRABR software. The FDR(DRP) component of FDRABR is used to restore the volumes. FDRDRP optimizes full volume recovery from ABR volume backups and eliminates the need for coding extensive restore JCL. Necessary information for performing the restores is retrieved from two sources, the ABR catalog and information from the tape management system that works with the FDRDRP software.

Make sure the STGSVOLS report and the SunGard DASD address chart are handy. The SunGard DASD address chart lists the disk addresses and indicates where each volume will be restored. The chart is prepared based on information provided in the SunGard-supplied Web-based mainframe test plan in the input box under the heading, Special DASD.

The following volumes are restored to IPL the system:

Volume	TSO Session	usercat	Started Tasks	Notes
ABRSYS	Y	.vpccx.		Already loaded during the load of FDRABR
TMS001				Used with ABRYSYS for DRP software
BOOKS1				
CICS00, CICS01, CICS03, CICS06, CICS10, CISC11, CICS14, CICS15				Required to bring up CICS regions. CICS00, CICS01, CICS14, CICS15 restored by FDR(DRP); CICS03, CICS06, CICS10, CICS11 restored by FDR/SUNCICS job.
DISR01, DIST00, DIST01, DIST02				Disaster Recovery volumes containing customer files, including profiles
HBL101				NHLBI Information System
JESCKA, JESCKB			JES2	
JESSP1, JESSP2, JESSRC			JES2	
LIB001	Y			
LIB002	Y	.pub5.		
LIB003	Y			
LIB016	Y			
LIB017		.pcc.		
LIB018	Y			
LIB019	Y			
MCATS4		master-cat		
MSTATS				Contains multiple libraries for software products (e.g., SAS, IRS, MARK IV)
MCATS9				
NIHLBA		usercat.nih		Should be at pre-determined UCB address since the address determines the IPL parameters
NIHLBB				Should be at pre-determined UCB address since the address determines the IPL parameters
NIHLBC				
NIHLBD	tmgr			
NIHLBE	shadow			
NIHLBF				
NIHLB1	Y			
NIHLB2	Y			
NIHLB3	Y			
NIHLB4				
NIHLB5				
NIHLB6				
OPSLG1, OPSLG2				
OPSLOG				
PAGE01				
PPCC12		.pub6.		
PPCC13				
RACFV1, RACFV2			RACF	
SHR001, SHR002, SHR003				
SMR001				
SYSOPS				Automated operations software
SYS4R1	Y			Should be at pre-determined UCB address since the address determines the IPL

Volume	TSO Session	usercat	Started Tasks	Notes
				parameters for system 4
SYS4R2	Y			
SYS4R3				
SYS9R1				Should be at pre-determined UCB address since the address determines the IPL parameters for system 9
SYS9R2				
SYS9R3				
UCATAG				
UCATHP				
UCATQZ				
UCAT01		.ucat01		
UCAT02		.ucat02		
UCAT03		.ucat03		
UCAT04		.ucat04		
UCAT05		.ucat05		
UCAT06		.ucat06		
UCAT07		.ucat07		
UCAT08		.ucat08		
UCAT09		.ucat09		
UCAT10		.ucat10		
WYL100				
DB2P01, DB2P02, DB2P03, DB2P04				DB2 SMS volumes, initialized only
DB2PS1, DB2PS2, SYSDB2, SSYDPR, OSSDB2, MASDB2, STGDB2				DB2 Non-SMS system volumes, initialized only
HSM101-71 HSMBC1 HSMBC2 HSMJRL HSMACD HSMOCD HSMPRM			Syshsm	HSM ML1 volumes HSM Control volumes
DSP101-189 DSL101-259 DSO010-107				SMS Managed Public volumes
SCR999				Non-SMS volume, initialized only. Must be at UCB address GENed as MSS, PUB, SYSDA, SYSSQ, SYSTS, and TMP.

The following database volumes are restored with the system volumes:

M204: M20401, M20402, M20403, M20404, M20405, M20406, M20407, M20408, M20409, M20410
IMS: IMS001, IMS002, IMS003, IMS004

The following user volumes are restored with the system volumes:

NIH: ODA103, ODA104, ODA105, ODA106 (Administrative Database)

NIH: OFM101, OFM102 (Central Accounting System)
 NIH: DRG001, DRG002, DRG003, DRG004, DRG005, DRG006 (IMPAC and CRISP)
 PSC: ESC101, ESC102, ESC103, ESC104, ESC105, ESC106 (DHHS Civilian Payroll System)
 PSC: FAF104 (Payment Management System)

Load DASD Using FDR(DRP) Software

1) Using ISPF EDIT (2):

```

EDIT                               NIH.STGADMIN.DIST.STARTUP.CNTL
Command ==>
      Name      Prompt      Size  Created
-----
      DRPJCL
      DRPJCLC
      DRPPARMA  *Edited      3    2005/07/20
      DRPPARMB      54    2006/05/05
      DRPPARMC     135    2006/05/05
      DRPPARMD      68    2006/05/05
      DRPPARME      80    2006/05/05
      DRPPARMF      72    2006/05/05
  
```

a) Submit member **DRPJCL** (sample JCL below).

b) Submit member **DRPJCLC**

Job Number _____, Time Submitted _____, Cond-Codes _____

Sample JCL:

```

//SG01DRP1 JOB 'TITAN RESTORE',CLASS=A,TIME=900,
// NOTIFY=SG01,MSGCLASS=D
//*****
//* FOLLOWING STEP ALLOWS DB2 TO BE RESTORED ALONGSIDE SUN BACKUPS  *
//* USE THIS JOB *ONLY* ON SUNGARD FLOOR SYSTEM                      *
//* RESTORE (PGM=FDRDRP) (V53. LEVEL59) USING 9840 TAPE DRIVES      *
//* ASSUMES: CATALOG VOLSER IS Z14CAT, NO OTHER CHANGES NEEDED    *
//* 11/15/04 DOB INCREASED REGION FROM 64M TO 0M                  *
//*****
//STEP1 EXEC PGM=FDRDRP,REGION=0M
//STEPLIB DD DSN=SUN1.FDRABR.LOADLIB,UNIT=3390,VOL=SER=Z14CAT,DISP=SHR
//SYSPRINT DD SYSOUT=*
//SYSPRIN1 DD SYSOUT=*
//SYSIN DD DSN=SG01.STARTUP.CNTL(DRPPARMA),DISP=SHR
/*
//*****
//* USE THIS JOB *ONLY* ON SUNGARD FLOOR SYSTEM                      *
//* RESTORE (PGM=FDRDRP) (V53. LEVEL59) USING 9840 TAPE DRIVES      *
//* ASSUMES: CATALOG VOLSER IS Z14CAT, NO OTHER CHANGES NEEDED    *
//* 11/15/04 DOB INCREASED REGION FROM 64M TO 0M                  *
//*****
//STEP2 EXEC PGM=FDRDRP,REGION=0M
//STEPLIB DD DSN=SUN1.FDRABR.LOADLIB,UNIT=3390,VOL=SER=Z14CAT,DISP=SHR
//SYSPRINT DD SYSOUT=*
//SYSPRIN1 DD SYSOUT=*
  
```

```
//SYSIN DD DSN=SG01.STARTUP.CNTL(DRPPARMB),DISP=SHR
/*
//
/* SUBMIT MEMBER DRPJCLC NEXT
```

NOTE: While the FDR(DRP) restore jobs are executing, you can restore the CICS volumes and initialize the public volumes while you are waiting.

- 2) **When the restore jobs have completed, enter the following command to verify that all required volumes (see previous table) have been restored and are on-line.:**

D U

Restore CICS Database Volumes

The FDR component of FDRABR is used to restore the database volumes of CICS.

Make sure the STGSVOLS report and the SunGard DASD address chart are handy.

The following CICS database volumes are to be restored: CICS03, CICS06, CICS10, CICS11

- 1) Using ISPF (3.4) DSLIST:

EDIT **NIH.STGADMIN.DIST.STARTUP.CNTL** on ABRSYS

Name	Size	Created	Changed	ID
_____SUNCICS	53	2001/10/08	2003/12/01	\$RYM

- 2) Select and edit member **SUNCICS**; and change if necessary: data set names, volume serial numbers, and unit addresses. Each Step will restore the CICS volume associated with it.

Submit the job, noting the times and job numbers. Verify job successfully complete (Cond-Code 0000).

Job Number _____, Time Submitted _____, Cond-Codes _____

If any of the jobs failed, they must be re-run after making appropriate adjustments before proceeding to the initialization of public volumes.

Initialize Volumes

Empty volumes will be initialized for DB2 and general public work space for DR testing.

- 1) Using ISPF (3.4) DSLIST:

EDIT **NIH.STGADMIN.DIST.STARTUP.CNTL** on ABRSYS

Members you will need:

Name	Size	Created	Changed	ID
____INIQUICK	99	2001/02/15	2002/03/12	\$RYM
____INITVVDS	65	2001/02/15	2002/03/12	\$RYM

Edit the **INIQUICK** member, sample JCL:

```
//SG01INI JOB ( ), 'FDR-LIBRARY', CLASS=A, TIME=15,
// MSGCLASS=D, NOTIFY=SG01
.
.
//*****
//*      NON-SMS VOLUME(S)                                *
//*****
//NSMS1   EXEC PGM=ICKDSF, REGION=6144K
//SYSPRINT DD SYSOUT=*
//SYSIN   DD *
        INIT      UNITADDRESS(4450) VERIFY(SG4450) VOLID(SCR999) -
                DEVTYPE(3390) INDEX(10,00,15) VTOC(11,00,60) -
                MAP NOCHECK NOVALIDATE
/*
.
.
.
.
```

Verify **all** of the INIT statements have correct UNITADDRESS, VERIFY, and VOLID parameters; the other parms will not change.

- 2) Before submitting the job, go to the Titan console and use the VARY command to take each of the volumes off-line, e.g.:

VARY 4480,OFFLINE (continue until all volumes have been taken offline)

- 3) Submit the job, and respond to each system prompt with:

nnU where nn = the number of the prompt

Wait for the job to successfully complete (Cond-Code 0000).

Job Number _____, Time Submitted _____, Cond-Codes _____

- 4) Go to the Titan console to use the VARY command to put each of the volumes on-line, e.g.:

VARY 380,ONLINE (continue until all of the nineteen have been placed back online)

- 5) Use the MOUNT command to mount all of the volumes, e.g.:

M 4480,VOL=(SL,DSL101)

- 6) Use the D U to verify the volumes are mounted, e.g.:

D U,,,4480,1

This will display the volume and where it is mounted.

IPL the System

IPL System 4 first, then System 9. The following instructions, with differences noted, apply to IPL'ing both LPARs.

****** IMPORTANT REMINDERS ******

Whenever any disk volumes are restored to one LPAR after both LPARs have been IPL'ed, the restored disk volumes MUST be varied offline and online on the other LPAR. If this is not done, any attempts to access the disk volumes on the other LPAR will fail.

If you need to re-IPL the system, shut the system down per the instructions below under *Shut Down the System*.

To logon from one of the Herndon PCs after the system has been IPL'ed, use the following command:

LOG APPLID(TSO*n*) where *n* is the system number (i.e., 4 or 9)

To retrieve Operator commands from the Herndon PCs that have been designated as the Titan Operator consoles, use the numeric keypad minus (-) key (located at the upper right corner of the numeric keypad).

- 1) Verify the load address and the load parameter.

<u>SYS4:</u> The load address must be the UCB address of the disk SYS4R1 and the format of the load parameter must be aaaa4DM where aaaa is the UCB address of the disk containing the IPLPARM and IODF data sets which reside on NIHLBB.
--

<u>SYS 9:</u> The load address must be the UCB address of the disk SYS9R1 and the format of the load parameter must be aaaa9DM where aaaa is the UCB address of the disk containing the IPLPARM and IODF data sets which reside on NIHLBB.

The addresses for these 3 volumes will always be:

SYS4R1 - xx02

SYS9R1 - xx03

NIHLBB - xx04

The 'xx' value will depend on the range of addresses assigned by SunGard. For example, if the address range is 78xx through 78yy, then the respective addresses for these volumes would be:

SYS4R1 – 7802

SYS9R1 – 7803

NIHLBB – 7804

The load address and load parms would then be:

SYS4 - Load address = 7802
Load parm = 78044DM
SYS9 - Load Address = 7803
Load parm = 78049DM

Provide the load address and the load parameter to the SunGard personnel.

- 2) The Operators will initiate the load.
- 3) The Master Console screen displays blue colored messages. Prompts pertaining to DASD volumes may appear. Respond accordingly.
- 4) The date and time on the console should be correct. If not, contact the SunGard personnel.
- 5) The Master Console screen should begin displaying green colored messages. You should see the following message regarding the sysplex environment:

IXC418I SYSTEM SYSX IS NOW ACTIVE IN SYSPLEX TITAN

The operating system will issue start commands for a number of Started Tasks (STCs).

- 6) After OPSMAIN4/OPMSMAIN9 initializes, it will issue the following WTOR, requesting directions pertaining to the activation of System State Manager (SSM):

nn SSMBEGIN ENTER DESIRED STATEMAN STARTUP OPTION (1-5) AND/OR MODE (A/P/I):

During the first IPL, place STATEMAN into PASSIVE mode. This will enable you to start the desired STCs and respond to WTORs without any interference from Automation. Issue the following response to place STATEMAN into PASSIVE mode:

R nn,1P

Note: Since OPSMVS is started with PASSIVE mode, all tasks will be started manually.

- 7) Issue the following command to disable all Time of Day rules in the TOD rule set:

OPSAOF disable TOD

- 8) The following commands SHOULD NOT be required to be issued unless there is a problem with the &PLACW system parameter which should be set to "DR". They are cited here for documentation purposes only:

OPSAOF disable MSG.\$HASP400
OPSAOF disable MSG.\$HASP426
OPSAOF disable MSG.IST051A

OPSAOF disable CMD.\$\$
 OPSAOF disable STD.EZZ4324I.
 OPSAOF disable STD.EZZ0403I.
 OPSAOF disable MSG.EZZ4324I.
 OPSAOF disable STD.SHADTOD
 OPSAOF disable STD.SHADTOD1
 OPSAOF enable STD.DR.

OPSAOF Resetauto MSG.\$HASP400
 OPSAOF Resetauto MSG.\$HASP426
 OPSAOF Resetauto MSG.IST051A
 OPSAOF Resetauto TOD

9) Start JES2.

The first time the system is IPL'ed, JES2 will have to be started manually because JES2 will have to be COLD started. All subsequent IPLs (such as bringing up System 9) will require a warm start.

Issue the following command:

SYS4: S JES2,DEV=DR,PARM=COLD	SYS9: S JES2,DEV=DR
--------------------------------------	----------------------------

The following non-highlighted message will appear on the console:

\$HASP400 ENTER REQUEST JES2 READY

After this message appears, issue the command to activate JES2: \$\$

The following printers are assigned to the Titan JES2 at the disaster site:

<i>Printer Model</i>	<i>Location</i>	<i>Printer Number</i>	<i>Unit Address</i>
3900	Reference test plan	PRT30	Reference test plan
4245	Reference test plan	PRT11	Reference test plan
4245	Reference test plan	PRT12	Reference test plan

Set the Unit Address for PRT30 by issuing the command:

\$TPRT30,UNIT=cuu

where cuu is the unit address obtained from the SunGard web-based test plan

- 10) If this is the initial manual IPL and JES2 is being cold started, issue the following command to also cold start ThruPut Manager:

SYS4: S TM,CF=COLD,CMF=COLD,VIF=COLD

Reply 'nnY' to the following messages.

DTM6007A IS A CONTROL FILE COLD START AUTHORIZED? REPLY 'Y' OR 'N'

DTM0805A IS A VIF COLD START AUTHORIZED? REPLY 'Y' OR 'N'

DTM7152A IS A DCS CMF FILE COLD START AUTHORIZED? REPLY 'Y' OR 'N'

The following messages will appear on the console:

DTM0023I TMSS INITIALIZATION COMPLETE
DTM6422I JLS RECONCILE COMPLETE
DTM7153I THE DCS CMF FILE IS BEING FORMATTED
DTM7154I THE DCS CMF FILE HAS BEEN FORMATTED (7200 BLOCKS, 600 TRACKS)
DTM2224I THRUPUT MANAGER VERSION 5 RELEASE 2.2 PTF TMT5212

After these messages appear, enter the following commands on the System 4 console:

%TM BATCH NIH.TMGRPROD.DRFOUR.COMMAND
%JAL EVENT ON DISASTER

Note 1: The first command defines a group of AGENT names and activates the agents on SYS4.

Note 2 (Important): The second command turns on a Thruput Manager 'Event' named DISASTER. When the DISASTER event is turned on, all jobs submitted by CA-7 are placed in 'Operator Hold' and are not executed. Jobs that are held by this facility can be released with the Thruput Manager command:

%JSS RELEASE 'JOBNAME'

or

%JSS RELEASE JES2 Job Number

If all jobs submitted from CA-7 are to be executed, issue the following command:

%JAL EVENT OFF DISASTER

To view the status of Thruput Manager events, issue the following command:

%JAL EVENT DISPLAY

SYS9: S TM

The following message will appear on the console:

DTM2224I THRUPUT MANAGER VERSION 5 RELEASE 2.2 PTF TMT5212

After this message appears, enter the following commands on system 9 console:

%TM BATCH NIH.TMGRPROD.DRNINE.COMMAND

%JAL EVENT ON DISASTER

Note 1: The first command defines a group of AGENT names and activates the agents on SYS9.

Note 2 (Important): The second command turns on a Thruput Manager 'Event' named DISASTER. When the DISASTER event is turned on, all jobs submitted by CA-7 are placed in 'Operator Hold' and are not executed. Jobs that are held by this facility can be released with the Thruput Manager command:

%JSS RELEASE 'JOBNAME'

or

%JSS RELEASE JES2 Job Number

If all jobs submitted from CA-7 are to be executed, issue the following command:

%JAL EVENT OFF DISASTER

To view the status of Thruput Manager events, issue the following command:

%JAL EVENT DISPLAY

All subsequent TM restarts on SYS4 and SYS9 will require a warm start using the following command:

S TM

11) Manually start the following tasks.

If this is the initial manual IPL, the SYSMIM and SYSMIA control file and checkpoints must be formatted as follows:

SYS4:

S SYSMIM,FORMAT=BOTH,

S SYSMIA,FORMAT=CF

SYS9:

S SYSMIM,FORMAT=CKPT

S SYSMIA

If this is NOT the initial manual IPL, then SYSMIM and SYSMIA may be started with the following on BOTH systems:

```
S SYSMIM
S SYSMIA
```

If this is an IPL of SYS4 and SYS9 is not up, the following message may be seen:

MIM0350W system SYS9 has not responded to CTC communication

This indicates that either SYSMIM or SYSMIA is waiting for a response that will not come because the other is down.

For SYSMIM, issue:

```
-FREE SYS9
```

For SYSMIA, issue:

```
_FREE SYS9
```

Issue the following commands:

SYS4:

```
S SLAMRUN
S TCPIP
S TN3270
S TCAS
S EMSPROC
S SYSVPSP
S SMR
S SRVVPSP
S DRSVPI
S GSSA
S BBVTAS.ZZUZPZO,SUF=P3
S BABCAS
S MVSPAS
S ENF
S NDMP
The Storage Group will start HSM
```

Note 1: After CCITCP and CCITCPGW are started, please inform TC Chen, so he can check their status.

Note 2: If SMTP does not come up because it is looking for data sets on public volumes, uncatalog all NIH.TCPIP.SMTP.* data sets and reissue the start command.

```
S SMTP
```

SYS9:

S SLAMRUN
S TCPIP
S TN3270
S TCAS
S BABCAS
S SMR
S MVSPAS
The Storage Group will start HSM

- 12) Issue the following command to start the NJE connection to production Titan (for tests only):

```
$SLGN1  
$SLINE(81)  
$SN,A=NIHJES2
```

NOTE: Make sure JES2 and Enterprise Extender are up and running before issuing this command.

- 13) **After both SYS4 and SYS9 are up, verify that all tape drives are online to both LPARs so that batch jobs won't hang or get cancelled.**

- 14) After all the above tasks have been started, CICS and M204 can be started. Notify appropriate staff to start these subsystems.

For the December 2 - 4, 2007 test, notify:
Ed Ryan at 301-496-1452 (CICS)
Hoyt Carelock at 301-435-5488 (M204)

- 15) DB2 and Oracle client

- a) Call either Ed Ryan at 301-496-1452, Angela Bennett at 301-435-5491, or Charles Green at 301-402-8523 to start DB2.
- b) If, prior to the backups that have been restored for the disaster recovery test, NIH.SHADOW.TITNSLK.SDBP.NIH.EXEC(SDBPIN00) had not been updated with the "emergency license code" for Shadow Direct, update the NIH.SHADOW.TITNSILK.SDBP.NIH.EXEC(SDBPIN00) to replace the LICENSECODE with the "emergency license code" obtained prior to the test.
- c) Verify that SYS9 is available.
- d) Start DSNP and the Oracle client on Titan by submitting the following job:

```
ZDB2DB2.CA7.DSNP.JCL(DB2PWSTR)
```

Note: This job issues an OPS message to Restart DSNP, and its related Oracle and Shadow jobs. At DR it will use the temporary license for Shadow Direct, so SDBP will

remain UP. However, at DR, Shadow Web Server - SWSP - will fail because there is no license. This is as planned since we do NOT want SHADSWSP executing at DR.

e) Perform a quick test of DSNP

f) Verify that SWSP is DOWN.

- 16) **IMS (SYS4 ONLY) – During DR tests, IMS is brought up manually via a COLD start.**
Since the IMS testing at the DR site does not involve accessing DB2, there is no need for DB2 to be started prior to starting IMS. If there are any problems starting IMS, please call Clyde Colmes at 301-496-6244 or Ed Ryan at 301-496-1452.

To bring up IMS during a DR test, always issue a COLD start as follows:

- a) Run batch job from IMSVS.V9R1.TITAN.P.SRCLIB(RCONREST)
- b) S IMS9DR
- c) When IMS puts out a WTOR "nn DFS810A IMS READY",
Enter: REPLY nn,/NRESTART CHECKPOINT 0 FORMAT ALL
- d) When you see "nn DFS996I *IMS READY* PROD" on the console log,
Enter: REPLY nn,/START TRAN IMS* JAH* IXX*
- e) When you see "nn DFS996I *IMS READY* PROD" on the console log,
Enter: REPLY nn,/START REG IMS9PMP8
- f) When you see "nn DFS996I *IMS READY* PROD" on the console log,
Enter: REPLY nn,/START DC
- g) When you see "nn DFS996I *IMS READY* PROD" on console log,
Enter: REPLY nn,/START LINE 3 PTERM ALL
- h) When you see "nn DFS996I *IMS READY* PROD" on console log,
Enter: REPLY nn,/START LINE 2 PTERM ALL
- i) S IMS9PRDR,MBR=JESCMDS1

APPC must be disabled at the DR site.

In order to avoid a repeat of the July, 2006 problem whereby some IMS users who signed on at NIH got the DR site instead (or vice versa), APPC must be disabled at the DR site.

The IMS proc for DR has been modified so that IMS at the DR site comes up with APPC disabled. To verify this:

- Logon to IMS at the DR site.

- Verify that you are connected at the DR site.
- Display APPC status via the /DIS APPC command.
- If APPC is enabled at DR, disable it with the /STOP APPC command.

An alternative is:

- Verify that IMS started OK at the DR site.
- Bring IMS down at the DR site.
- The next morning, after IMS has been started at NIH, restart IMS at the DR site.
- Logon to IMS at the DR site.
- Verify that you are connected at the DR site.
- Display APPC status via the /DIS APPC command.
- If APPC is enabled at the DR site, disable it with the /STOP APPC command.

The procedures for an IMS warm start are included here for documentation purposes only:

- a) S IMS9DR
- b) When IMS puts out a WTOR "nn DFS810A IMS READY",
Enter: REPLY nn,/NRESTART
- c) When IMS puts out a WTOR "nn DFS996I *IMS READY* PROD" then,
Enter: START IMSVTAM
- d) You will see "nn DFS996I *IMS READY* PROD" on the console log,
Enter: REPLY nn,/START TRAN IMS* JAH* IXX*
- e) You will see "nn DFS996I *IMS READY* PROD" on the console log,
Enter: REPLY nn,/START REG IMS9PMP8
- f) You will see "nn DFS996I *IMS READY* PROD" on the console log,
Enter: REPLY nn,/START DC
- g) When you see "nn DFS996I *IMS READY* PROD" on the console log,
Enter: REPLY nn,/START LINE 3 PTERM ALL
- h) When you see "nn DFS996I *IMS READY* PROD" on the console log,
Enter: REPLY nn,/START LINE 2 PTERM ALL
- i) S IMS9PRDR,MBR=JESCMDS1

SYSHSM

All volumes necessary for production SYSHSM have now been restored and all Disaster Tape volumes have been transported to the Disaster site.

Do the following to bring up SYSHSM at the DR site.

- 1) Edit Syshsm.parmlib(arccmd04):

Insert the following: SETSYS DISASTERMODE
Change setsys DUPLEX to NO for both Backup and Migration
Add the Hold All to the end of arccmd04

- 2) Start SYSHSM
- 3) Verify that Initialization completed successfully; correct any errors.
- 4) Once Initialization is complete, issue: TSO HSEND RELEASE TAPEREPL
- 5) Issue: TSO HSEND TAPEREPL ALL DAVOLUMES
- 6) Issue: TSO HSEND RELEASE RECALL
- 7) Test Recall of a dataset on ML2. If the subsequent tape mount calls for a H2* volume, then Syshsm is functional.
- 8) Issue: TSO HSEND RELEASE ALL
- 9) Issue: TSO HSEND HOLD BACKUP MIGRATION (For DR Test only)

In the event of a real Disaster all H2* should be available. It will be necessary to reconcile the H2 tapes currently in use with those H2 tapes available as HSM scratch tapes.

Issue TSO HSEND LIST TTOC ODS('\$DOB.TTOC.ALL.JAN21A') DSI from the TSO command line of from ISPF 6.

Edit the Output dataset. Sort the data by cols 2-7. Any tape number not listed needs to be added to HSM via the Addvol command as either a Backup or Migration tape as needed.

See DFSMSHsm Storage Administration Reference for details. It is available on Bookmanager.

Workload Manager (WLM)

Once the system is IPL'ed and TSO is available, the standard Titan Workload Manager policy (TTANSTD) can be installed into the WLM DR couple datasets and activated. Until that is done, an IBM default policy will be in effect and not conducive to our system environment as activity picks up.

Do the following to install TITANSTD:

- 1) Logon to TSO and go into the ISPF command screen (6).

- 2) Enter: EX 'SYS1.SBLSCLI0(IWMARIN0)'
- 3) Select "Read Saved Definition", from NIH.WLM.SYS4DR.PDS
- 4) Select "Install" from the "Utilities" bar at the top.
- 5) Select "Activate" from the "Utilities" bar at the top.
(An alternative would be the console command: V WLM,POLICY=TITANSTD)
- 6) Select "Exit" from the "File" bar at the top.

You can double-check for our policy TITANSTD activation using the console command:

```
D WLM,SYSTEM=SYS4
```

Note: This is SYSPLEX-wide, and will also be in effect on SYS9 if it is up – or when it does come up.

Manual START Commands

In case you need to manually start various tasks, Section 9 of the Titan System Programmers Handbook should have most of the information you need to do this.

To see how OPS/MVS would normally bring up a started task, begin by looking at the data set SYS1.SYSn.PROCLIB(OPSMAlNn) where "n" is the system in question. Then look at the data sets allocated to the SYSEXEC ddname. Look for member names beginning with the string "START...". Then look for the text "issue" and you will generally be close to the command that OPS/MVS would issue. To see how OPS/MVS would stop the task, look at the member names beginning with "STOP...".

Shutdown Procedures

Shut Down the System

- 1) Before shutting down the system, DB2 needs to be terminated as follows:

Call the DB2 support person to submit the following job for stopping DSNP and the Oracle client on Titan.

```
ZDB2DB2.CA7.DSNP.JCL(DB2PWSTP)
```

Note: Initiator must be available before executing the job.

- 2) Issue the following command on the console for the system you are shutting down:

```
SHUTDOWN ENTIRE SYSTEM NOW
```

- 3) Reply “U” to “accept”, then “N” to “shutdown now” in response to SSMSHUT request from OPS System State Manager.
- 4) Reply “5” to SSMBEGIN start option to select the “Use current desired state and no schedule” option.
- 5) After started tasks are terminated, if the other system is still up, issue

VARY XCF,SYSn,OFFLINE

where n = 4 or 9, the number of the system you are shutting down. This removes the system from the Sysplex.

- 6) Reply “SYSNAME=SYSn” (where n = 4 or 9) to message IXC371D “Confirm request to vary system offline”.
- 7) Reply “DOWN” to message IXC102A “XCF is waiting for system SYSn deactivation” on the other system.

Shut Down IMS

Use the following procedure in TSO Option 'S.OPS' (AutoOps):

- 1) Issue the following operator command to get the number of the Outstanding IMS message:

/D R,L

The following example is the response from the July 2005 test:

```
20JUL 15:13:10 D R,L
20JUL 15:13:10 IEE112I 15.13.10 PENDING REQUESTS 742
20JUL 15:13:10 RM=7 IM=0 CEM=0 EM=0 RU=0 IR=0 NOAMRF
20JUL 15:13:10 ID:R/K T TIME JOB ID MESSAGE TEXT
20JUL 15:13:10 97 R 15.11.38 04S17361 *97 DFS996I *IMS READY* TEST
```

- 2) Issue the following operator command to display active the IMS regions:

97/dis a

The following example is the response from the July 2005 test:

```
R 97,/DIS A
IEE600I REPLY TO 97 IS:/DIS A
DFS000I REGID JOBNAME TYPE TRAN/STEP PROGRAM STATUS
DFS000I 2 IMS7TMP1 TPE WAITING
DFS000I 1 IMS7TMP5 TPE WAITING
DFS000I JMPRGN JMP NONE
DFS000I JBPRGN JBP NONE
DFS000I BATCHREG BMP NONE
```

```
DFS000I    DBTRGN DBT NONE
DFS000I    IMS7TRC DBRC
DFS000I    IMS7TSAS DLS
DFS000I    VTAM ACB OPEN      -LOGONS ENABLED
DFS000I    IMSLU=NIH.APPCIMST  APPC STATUS=ENABLED TIM
DFS000I    OTMA GROUP=N/A     STATUS=NOTACTIVE
DFS000I    APPLID=IMSTEST GRSNAME=    STATUS=DISABLED
DFS000I    LINE ACTIVE-IN - 1 ACTIV-OUT - 0
DFS000I    NODE ACTIVE-IN - 0 ACTIV-OUT - 0
```

3) Issue the following command to stop an IMS region:

/mm/STOP REGION n (where mm is the new outstanding message id and n is the region ID)

The following example is from the July 2005 test.

```
R 98,/STOP REGION 2
IEE600I REPLY TO 98 IS:/STOP REGION 2
DFS058I 15:13:44 STOP COMMAND IN PROGRESS
DFS058I 15:13:44 STOP COMMAND IN PROGRESS TEST
99 DFS996I *IMS READY* TEST
DFS552I MESSAGE REGION IMS7TMP1 STOPPED ID=00002 TIME=1513 TEST
DFS552I MESSAGE REGION IMS7TMP1 STOPPED ID=00002 TIME=1513
```

Other Vendor Software

The following products have licensing restrictions that require special procedures to enable them to run at the hot site:

Connect:Direct

Connect:Direct requires a new license key. Contact https://support.sterlingcommerce.com/forms/connect_key_request.aspx or call customer support at 1-800-292-0104 to obtain a license key to update the data set APDSN with the hot site cpu ID. The DCSS customer ID is 11653.

IOF

IOF requires an authorization patch. Contact Patty Robbins (patty.robbins@triangle-systems.com) and Christine Cargnoni (Christine.cargnoni@fisc.com) to obtain the patch. When making the request be prepared to provide the following information:

- Starting day of test and length (3 days)
- Current IOF release level: 7.G.0
- Processor type being emulated at the hot site: 9672-RB6
- Product license and issuer: 085 0693, Federal Data Corporation
- CPU ID and machine type: obtained from the SunGard web-based test plan

The following is an example of the patch that will be received:

```
REP 00 10C9,0F57,B68C,B165 - good thru 07 Nov 2001, Wednesday
```

- 1) Member A40EXPIR in NIH.IOF.PROD.IOFT7GO.OPTIONS must be updated with the new zap codes; examples of the format are in the member.
- 2) Execute member M40EXPIR in NIH.IOF.PROD.IOFT7GO.INSTALL.
- 3) If condition code 0 is returned, do an LLA Refresh (F LLA,REFRESH) to activate the new authorization code.

MAX

MAX software requires temporary enabling codes (good for 10 days). Contact the vendor at 1-888-376-6629 or 301-985-1558, or by email, info@maxsoftware.com to request the authorization zaps. Indicate the request is for NIH (CIT) for testing at SunGard on the specified test dates and provide the SunGard CPU serial number and processor type/model number (obtained from the SunGard web-based test plan).

- 1) Make sure the DR passwords are in the MAXAUTH member in the NIH.MXRX320.JCL library.
- 2) Submit ASMAUTHS from the NIH.MXRX320.JCL library to create the MAXAUTH load module.
- 3) If the jobs are run after the system has been IPL'ed, do an LLA Refresh; otherwise, wait for an IPL.
- 4) Verify the Max functions (Max View, Max Edit, Max PDF, Max Utility) are accessible without an authorization error message. Submit a batch job executing pgm=maxbat to ensure that it executes without error.

**MIA
MIM
OPSMVS
SMR
TMS**

These products require an authorization key. Contact Computer Associates (CA) at 1-800-338-6720 to request the authorization key. Provide the site ID: 193082 and the CPU ID and model number of the SunGard system (obtained from the SunGard web-based test plan). The EKG key received from CA is put into the KEYS member of PPOPTION.

Model 204

Contact Liz Klass of CCA at 703-506-2107 to obtain the cpuzap for the disaster recovery site. You will need to provide the CPU ID and the operating system level (obtained from the SunGard web-based test plan). Create a new copy of NIH.M204.RACF.PGMS.DISASTER and apply the zap to the new copy (the dataset is on M20402) as follows.

Prior to the test, on the home production system:

- 1) Logon to TSO and copy the NIH.M204.RACF.PGMS to another

dataset - NIH.M204.RACF.PGMS.DISASTER.

- 2) Use SPF 3.3 to copy ONLINE, IFAM1, IFAM4 and Batch204 modules into the NIH.M204.RACF.PGMS.DISASTER library.
- 3) Upload the CCA zap to the dataset \$DBS.HOTSITE.ZAP.
- 4) Run the job NIH.M204.V510.FIXES.DATA(ZAPUCPU) to zap/update ONLINE, IFAM1, IFAM4 and Batch204 modules, which are stored in the NIH.M204.RACF.PGMS.DISASTER library. This zap verifies and then replaces the CPU name info with 0000's; thus removing the present NIH site information.
- 5) Run the job NIH.M204.V510.FIXES.DATA(ZAP510) to zap/update ONLINE, IFAM1, IFAM4 and Batch204 modules, which are stored in the NIH.M204.RACF.PGMS.DISASTER library. This zap verifies and then replaces the 0000's with the hot site cpu information.

At the hot site:

- 1) Logon to TSO SPF.
- 2) Use SPF 3.3 to copy the ONLINE, IFAM1, IFAM4 and Batch204 modules from the NIH.M204.RACF.PGMS.DISASTER library to the NIH.M204.RACF.PGMS library.
- 3) Start M204PROD by entering the following at the console:

/S M204R

Quick-Ref

Quick-Ref requires a key to run at the DR site. Contact Chicago-Soft at 733-282-4777 or by email: zap@chicago-soft.com to obtain the keys. You will need to provide the following information: the key is for the US National Institutes of Health, LA #9011495, the date of the test, and the CPU ID.

Run the job NIH.QUICKREF.R640.JCL (QWIEXPDT) to apply the zap to member QWIKREF1 in the current Quick-Ref linklib.

SAS

To prepare SAS PROCs for use in a DR situation, comment out the two DD cards containing DSN=SYSDB2 in each of the following two PROCs: ZABCRUN.PROCLIB (SAS) and ZABCRUN.PROCLIB (SAS609). The SAS PROCLIB resides on MSTATS.

Contact Mr. Ray Danner at (301)496-6037 or Ms. Cindy Harper at (919)677-8000 to obtain a SETINIT job. Execute the SETINIT job after modifying the SAS PROCs. This will suppress printing of the SAS

warning messages.

It is not necessary to obtain the SETINIT job for hot site testing, but SAS should be notified after the test.

Shadow

Shadow requires a temporary “emergency license code”. Contact Neon Systems by email: support@neonsys.com.

Superset Utilities

Superset Utilities require authorization codes. Contact Applied Software (Ron Turner) at 215-297-9441, Fax 215-297-9498, or by email: ron@appliedsoftware.com to request the authorization codes. Provide the dates, CPU serial number, and model number of the SunGard system (obtained from the SunGard web-based test plan).

Assuming module AS0000PW is already prepared with the authorization codes, you can use the following shortcut procedure from the floor system prior to the first IPL:

Use ISPR 3.3 “Move/Copy Utility” to REPLACE module AS0000PW:

From: ‘NIH.SUPERSET.DR.LOAD’, Volume ABRSYS

To: ‘SYS1.SUPERSET.LOAD’, Volume NIHLBB

Be sure to specify “/” to allow “Replace like-named member”

If you did not use the pre-IPL procedure above, do the following:

The two members in NIH.SUPERSET.DR.CNTL for updating the authorization module are: ASMPSWDX and PCCPSWDC. Make sure PCCPSWDC has the current authorization codes. Edit member ASMPSWDX to make sure “//SYSLMOD” points to library SYS.SUPERSET.LOAD submit the job.

After the batch job completes, optionally browse SYS1.SUPERSET.LOAD(AS0000PW) to verify the current disaster site codes are in place.

From the console:

F LLA,REFRESH

Products requiring keys to run at the DR site and responsibilities:

VENDOR	PRODUCT	KEY REQUIRED FOR DR TEST?	RESPONSIBLE
Applied Software, Inc	Superset utilities	yes	S Filbert
BMC Software	CMF Monitor		B Long
	Loadplus		E Ryan
	Mainview		B Long

	Resolve/Sysprog		B Long
Chicago Soft	Quick-Ref	yes	B Bauer
Computer Associates	CA1		D O'Brien
	CA7		TC Chen
	CA11		TC / J Dussault
	Common Service		TC / J Dussault
	MIA/MIM		B Bauer
	OPSMVS		TC / J Dussault
	SMR	yes	TC / J Dussault
	TMS	yes	TC / J Dussault
Computer Corp. of America	Model 204	yes	H Carelock
DataDirect Technologies	Shadow z/Direct	yes	E Ryan
	Shadow z/EnterpriseWeb Server		E Ryan
Fisher Int'l Sys., Inc.	IOF	yes	B Long
Max Software	MAX	yes	C Green
SAS Institute	SAS	yes	A Bennett
Software Engineering of America	PDSFast		B Long
Sterling Commerce	Connect:Direct	yes	B Bauer G Tran

Dump Disaster Volumes

After the completion of disaster recovery testing, the disaster volumes, DIST00, DIST01, and DIST002 are dumped to 9840 scratch tapes to be returned to NIH.

The NIH.STGADMIN.DIST.WORK.CNTL(DISTDUMP) dataset contains the JCL to perform the dumps. The only changes to the JCL that may be necessary might be the volume serial numbers of the volumes being dumped and the tape device parameters.

Submit this job (after any necessary edits), noting the job number and time, and verify successful completion (Cond-Code 0000).

Dump Console Log Volumes

As long as SMR has been running during the test, the current day's console logs will be in data sets named NIH.CA.SYSLOG.CURRssss where "ssss" is the SMFid of the system (e.g., 4090). The log for the previous day will be in the data set named NIH.CA.SYSLOG.SMRyyjjj where "yy" is the last 2 digits of the year and "jjj" is the Julian date. You should verify that these data sets are on NIHLB4 and SMR001 respectively. If not, modify the JCL below as necessary.

After the completion of disaster recovery testing, the volumes NIHLB4 and SMR001 containing the console logs are dumped to 3490 scratch tapes to be returned to NIH.

The NIH.STGADMIN.DIST.WORK.CNTL(DUMPLOGS) dataset contains the JCL to perform the dumps. The only changes to the JCL that may be necessary are the volume serial numbers of the volumes being dumped and the tape device parameters.

Submit this job (after any necessary edits) and verify successful completion (Cond-Code 0000). Also make a note of the scratch tapes that were written so that you can copy these tapes once the "scratch" tapes come back to NIH. You must use DFDSS to copy these tapes (for sample JCL, see \$JDA.DISASTER.CNTL(COPYDUMP)).

Miscellaneous

The following is useful information.

SMF

From time to time it may be necessary to clear the SMF datasets on the DR z/OS operating system. The following procedure can be used to manage the SMF data.

- 1) On the Operator's console issue the 'D SMF' command. This displays the status of the SYS1.MAN1, SYS1.MAN2, and SYS1.MAN3 datasets.
- 2) If any of the MAN files shows a status of 'DUMP REQUIRED' the job SMFCLEAR can be submitted from dataset NIH.DISASTER.JCL. Be sure to specify the MAN file you wish to clear (1,2, or 3) on the EXEC card. This job will clear all records from the SMF MAN file and reset it back to 0% full."

CICS

- 1) Since the environment at the DR site is new and the log streams will be defined for this new environment, the CICS startup should be INITIAL. The easiest way to achieve this is by adding the following to the SIT override data set, i.e., adding to NIH.CICSTS22.PROD.R1CICS22.SYSIN(DFH\$SIPT) :

START=INITIAL, X

- 2) Since TMON for CICS is not started at the DR site, CICS will not start at the DR site unless the TMON programs that it executes during its initialization at NIH are removed from the initialization at the DR site. The easiest way to achieve this is by adding the following to the SIT override data set, i.e., NIH.CICSTS22.PROD.R1CICS22.SYSIN(DFH\$SIPT) :

PLTPI=NO, X

- 3) UNCATLOG, DELETE and DEFINE the logstreams for CICS:

Verify that you are logged in at the DR site (System 4).

Verify the names of the CICS log data sets referenced in
NIH.CICSTS22.PROD.R1CICS22.LIBRARY(LGRUNCAT).

Note: The generation qualifier in the data set names referenced in LRGUNCAT change from one DR test to the next.

Modify LGRUNCAT based on the log datasets that are cataloged at the DR site.

Note: Prior to submitting the LGRUNCAT JCL, you may want to recall any datasets that you will uncatalog that are currently migrated. If you don't, it may take a long time for the LGRUNCAT job to execute as recalls of migrated datasets at the DR site seem to be longer than normal.

Note: To execute LGRUNCAT you need ALTER access to:
PRF.CP1.PPCSPROD.USRJRNLS.**
OFM.HAS.FDMSPROD.USRJRNLS.**
OFM.HAS.PCAPROD.USRJRNLS.**

Note: ZDB2EOR has the required access authority.

Remove the comments from the job card, and execute LGRUNCAT.

Note: A cond code = 8 may be alright; just verify that the log files are uncataloged.

From OPSLOG, display the logstreams by issuing:

```
/d logger,logstream
```

As an alternative, the logstreams can be displayed from the IOF LOG with the following command:

```
#d logger,logstream
```

Modify NIH.CICSTS22.PROD.R1CICS22.LIBRARY(LGRDELETE) based on the CICS logstreams that do not exist at the DR site. Many, if not all, of the logstreams may not initially exist at the DR site. Remove any CICS logstreams that do not exist at DR because their presence in the JCL will cause the submission to receive a Cond Code = 0012. If none of the CICS logstreams initially exist at the DR site, there should be no need to execute LGRDELETE.

Remove the comments from the job card, and execute LGRDELETE.

Note: To execute LGRDELETE, you need READ access to: MVSADMIN.LOGR cl(facility).
ZDB2EOR has the required access authority.

Remove the comments from the job card, and execute
NIH.CICSTS13.PROD.R1CCIS22.LIBRARY(LGRDEFIN).

- 4) If CICS06 and CICS11 have not yet been restored, comment out the DTM loadlib from the RPL. (CCIS11 contains the file and CICS06 contains the catalog).

- 5) Bring up the region by issuing the following command:

```
/S CICS22R1
```

- 6) Verify that the user files are allocated to CICS.

- 7) If the user files are not allocated, you may need to execute the following transactions:

```
AARM  
ADMC  
APCA
```

- 8) Modify the record in NIH.CICSTS22.SITEFILE to a '2'.

- 9) Test the Site transaction.

- 10) Issue the following command:

```
CECI EXEC CICS LINK PROG('DUMPTBLE')
```

- 11) Notify the staff at the DR site that CICSPROD is up.

TESTING THE Oracle Client

- 1) Log on to DRTITAN2.NIH.GOV (System 9).
- 2) Verify the contents of the SQLNET and Oracle TNSNAMES files.

Note: There is a current project in CIT to discontinue support of Oracle Names. Until this project is completed:

- Verify that any customer testing at the DR site who has already transitioned to using their own SQLNET and TNSNAMES files, modifies the entries in their TNSNAMES file to point to the databases at the DR site.
- Continue with the following steps if there are DR customers who are testing and have not yet transitioned to their own SQLNET and TNSNAMES files.

The ORASQL, ORALDR, and ORACB2 procs in the NIH.ORACLE.PROCLIB each contain the following DD cards:

```
//sqlnet dd dsn=nih.sqlnet.ora,disp=shr  
//tnsnames dd dsn=nih.oracle.tnsnames,disp=shr
```

At the NIH, the directory path in NIH.SQLNET.ORA looks first at TNSNAMES and then at ONAMES. On Titan, NIH.ORACLE.TNSNAMES has no entries, so unless the JCL overrides the TNSNAMES DD statement in the proc by specifying a different TNSNAMES data set that contains entries, the connection at the NIH is made using ONAMES. The ONAMES entries point to the NIH computer systems.

Note: AFPSP, John Biggie's application, uses NIH.SQLNET.ORA.ASO instead of NIH.SQLNET.ORA, but the process is the same.

During disaster recovery, the users' connections should not be to the NIH machines. The connections should be to the machines set up at the disaster recovery site. The connections to REPOSPRD that are made to test the members of NIH.ORACLE.PROCLIB are made to the database back at NIH.

The connection information needed at the DR site is contained in NIH.SQLNET.ORA.DRSITE, NIHSQLNET.ORA.ASO.DRSITE, and NIH.ORACLE.TNSNAMES.DRSITE. The job, DB2PWSTR, starts ORAONSP at the disaster recovery site. The job includes steps that copy NIH.SQLNET.ORA.DRSITE, NIHSQLNET.ORA.ASO.DRSITE, and NIH.ORACLE.TNSNAMES.DRSITE to NIH.SQLNET.ORA, NIH.SQLNET.ORA.ASO, and NIH.ORACLE.TNSNAMES, respectively. When NIH.SQLNET.ORA, NIH.SQLNET.ORA.ASO, and NIH.ORACLE.TNSNAMES are referenced at the DR site, they contain the connection information needed for the test; not the connection information used at NIH.

- 3) Verify the absence of numbering in NIH.ORACLE.TNSNAMES, NIH.SQLNET.ORA.ASO, and NIH.SQLNET.ORA. To do this, edit NIH.ORACLE.TNSNAMES, NIH.SQLNET.ORA.ASO, and NIH.SQLNET.ORA and press PF11. If there are numbers on right, go to the command line and enter the UNNUM command.
- 4) Verify that the TMX11826I message references the IP address at the DR site.
- 5) Verify the TCP/IP connections. From TSO enter:

PING DREOS.CIT.NIH.GOV
- 6) The following are problems from previous tests with resolution. They are included here in case they occur during current testing; this may help hasten the resolution.

Problem	Solution
The job just waited on the execution queue	The ORACLE JES2 agent needed to be activated
The TNSNAMES and ORACLE NAMES files had numbers on and extraneous data in the right most columns of the data sets	The UNNUM command needed to be issued on the files
Job submission errors stating: Temporary control card data set cannot be allocated DAIR RC = 12 dec, DARC = 970C hex	The resolution was to UNCATALOG the ZDB2INI.SYS4...CNTL data set

7) Test the Oracle procs

If space on EOS is limited at the DR site (this is usually the case), NIH.ORACLE.TNSNAMES.DRSITE will have an entry for REPOSPRD which connects to REPOSPRD at the NIH. If so, the password for the test of REPOSPRD must match the password on EOS at NIH.

Prior to testing verify that:

- The directory path in NIH.SQLNET.ORA does not include ONAMES,
- The directory path in NIH.SQLNET.ORA.ASO does not include ONAMES, and
- the DR entries are included in NIH.ORACLE.TNSNAMES.

Test ORASQL and ORALDR

a) Submit the following JCL:

```
ZDB2INI.ORA.TJS.REPOSPRD.JCL(SQLPLUS)
```

b) If the SELECT succeeded (the tjs_table1 exists), execute the following:

```
ZDB2INI.ORA.TJS.REPOSPRD.JCL(DELROWS)
ZDB2INI.ORA.TJS.REPOSPRD.JCL(SQLLOAD)
ZDB2INI.ORA.TJS.REPOSPRD.JCL(SQLPLUS)
```

c) If the SELECT failed (the tjs_table1 does not exist), execute the following:

```
ZDB2INI.ORA.TJS.REPOSPRD.JCL(CREATETB)
ZDB2INI.ORA.TJS.REPOSPRD.JCL(SQLLOAD)
ZDB2INI.ORA.TJS.REPOSPRD.JCL(SQLPLUS)
```

Test ORACB2

a) Submit the following JCL:

```
ZDB2INI.ORA.TJS.REPOSPRD.JCL(COBOLCL)
```

b) Add //TNSNAMES DD NIH.ORACLE.TNSNAMES,DSP=SHR to
ZDB2INI.ORA.TJS.REPOSPRD.JCL(COBOLGO)

c) Enter: EXECUTE 'ZDB2INI.ORA.TJS.REPOSPRD.JCL(COBOLGO)'

8) Verify the connection to AFPSP at the DR site:

a) On the Database Development Main Menu, enter: O

b) You will be prompted for the fully qualified TNSNAMES file.
Enter: NIH.ORACLE.TNSNAMES

c) You will be prompted for the Oracle Connect String.
Enter: REPOSPRD.WORLD

- d) You will be prompted for your Oracle userid.
Enter: ZDB2INI
 - e) You will be asked to confirm the TNSNAMES file, connect string, and userid.
Press Enter to confirm or enter NO to repeat the prompt cycle.
 - f) After confirming the information, you will be prompted for the password.
Enter the password.
 - g) The SQL prompt is displayed.
Enter: HOST TNSPING AFPSP.WORLD
 - h) If AFPSP has been restored at DR, the host will be identified as DREOS.CIT.NIH.GOV.
- 9) Using the ORAMON userid, test the connection to AFPSP at the DR site.
- Verify the password in ZDB2INI.ORA.TJS.REPOSPRD.PARMLIB(AFPSP).
Submit ZDB2INI.ORA.TJS.REPOSPRD.JCL(AFPSP).
- 10) Call the disaster recovery site to report that all is okay.

TESTING DB2

The DB2 disaster recovery testing plan is in ZDB2DB2.DR.DB2.CNTL(TESTING).

FDR/ABR Model

Procedures to place an FDR/ABR Model on a volume. Either edit and submit the batch job in NIH.STGADMIN.DIST.WORK.JCL(INIMODEL) or do the following.

- 1) On the Command line of the main ISPF panel, select option **C**, Products, and hit the enter key.
- 2) On the Command line enter **A.I.8** and hit the Enter key. The following panel will be displayed. If the dataset name indicated in bold is not the one displayed, type it in. Hit the Enter key.

ABR DISK VOLUME PROCESSING OPTIONS MUST BE SET PRIOR TO ABR EXECUTION.
SETTING THE ABR PROCESSING OPTIONS DOES NOT AFFECT NORMAL USE OF THE VOLUME.

FDR PROGRAM LIBRARY DATA SET:
DATA SET NAME ===> 'SYS1.FDRABR.PROD5359.LINKLIB'
VOLUME SERIAL ===>
SYSOUT CLASS ===> *

JOB STATEMENT INFORMATION:
===> //STGMODEL JOB (ZZXZ,112,E), 'COLLINS,NOTIFY=\$RYM

```

===> /*ROUTE OUTPUT HOLD
===> /*
===> /*

```

PLEASE PRESS THE "ENTER" KEY TO DISPLAY THE TABLE

-----COPYRIGHT 1987, 2000 --- INNOVATION DATA PROCESSING, INC.-----

- 3) The panel to create the ABR Model will be displayed. Enter DASD volser under the Volume Serial Number column (as indicated in bold) and hit the enter key.

```

-----FDR INSTALLATION -- SET ABR VOLUME PROCESSING OPTIO Row 1 to 1 of 1,
COMMAND ===>                                SCROLL ===> PAGE

```

```

SUBMIT - SUBMIT FDRABRM BATCH JOB      EDIT - EDIT FDRABRM BATCH JOB
REFRESH- REFRESH ABR VOLUME INFO      FIND - FIND THE SPECIFIED STRING

```

```

      ----CURRENT BACKUP-----
      VOLUME GEN CYC  EXPDT  AC MOD  MAX GEN  RETPD  ARCHIVE  STORCLAS  FORCE
      SERIAL  DATE    EXPD2          MAX AC  RETP2  SCRATCH  ARCHI
CMD  NUMBER
---  -----
      DDDXXX
---  -----
PLEASE ENTER THE VOLUME SERIAL NUMBERS TO DISPLAY/SET ABR PROCESSING OPTIONS

```

- 4) The values set for volume DSL101 will be displayed:

```

-----FDR INSTALLATION -- SET ABR VOLUME PROCESSING OPTIO Row 1 to 1 of 1,
COMMAND ===>                                SCROLL ===> PAGE

```

```

SUBMIT - SUBMIT FDRABRM BATCH JOB      EDIT - EDIT FDRABRM BATCH JOB
REFRESH- REFRESH ABR VOLUME INFO      FIND - FIND THE SPECIFIED STRING

```

```

      ----CURRENT BACKUP-----
      VOLUME GEN CYC  EXPDT  AC MOD  MAX GEN  RETPD  ARCHIVE  STORCLAS  FORCE
      SERIAL  DATE    EXPD2          MAX AC  RETP2  SCRATCH  ARCHI
CMD  NUMBER
---  -----
      DDDXXX                xxx    xx    xx    xxx    xx    xxx
                                xx    xx    xxx    xx
                                xx    xx    xxx    xx
---  -----
***** Bottom of data *****

```

Either accept the values or change as appropriate.

- 5) At the COMMAND ===> prompt, enter: SUBMIT, followed by the Enter key. This will submit the batch job for the selected ABR model.
- 6) Either use IOF to display the batch job to verify the ABR model has been created or:

Using IPSP (3.4) DSLIST:

Data Set List Utility

Option ==>

Blank Display data set list

P Print data set list

V Display VTOC information

PV Print VTOC information

Enter one or both of the following parameters:

Dsname Level: **FDRABR.***

Volume Serial: **DDDDXXX**

Hit the Enter key; the following will be displayed:

DSL1ST - Data Sets on volume DSL101

Row 1 of 1

Command ==>

Scroll ==> PAGE

Command - Enter "/" to select action

Message

Volume

FDRABR.VDDDDXXX

DDDDXXX

SunGard Esoterics

<i>Device Type</i>	<i>Esoteric</i>
3380 and 3390	SYSDA, DISK, SYSSQ
3420	TAPE
3480	CART and TAPEC
3490	CART3490 and CARTE
MetroCenter 3420	METRO20
MetroCenter 3480	METRO
MetroCenter 3490	METRO90
3480 and 3490	ALLCART
3590 - All Models	CART3590, MAGSTAR
3590B	CART359B
3590E	CART359E
3590H	CART359H
9840 - All Models	CART9840, STK9840
9840C	STK9840C
9940B	STK9940, CART9940
3494-B18 / 3490E	VTs
3494-B18 / 3590E	ATL
STK VSM	VSM

Appendix F2 – EOS Restore Procedures

Tru64 5.1B

Last Modified: 7/16/07

Network information

dreos.cit.nih.gov	165.112.213.240	drzinc.cit.nih.gov	128.231.164.19
default router	165.112.213.225	default router	128.231.164.17
netmask	255.255.255.224	netmask	255.255.255.248
drgarnet.cit.nih.gov	128.231.164.11	drlapis.cit.nih.gov	128.231.164.3
default router	128.231.164.9	default router	128.231.164.1
netmask	255.255.255.248	netmask	255.255.255.248
drtn3270.titan.nih.gov	165.112.213.229		
zinc.cit.nih.gov	128.231.19.214		
eos.nih.gov	128.231.56.102		
garnet.cit.nih.gov	128.231.56.132		
lapis.cit.nih.gov	128.231.56.128		

DR Website

<http://dr.cit.nih.gov> Viewing status
<http://dr.cit.nih.gov/drentry.cfm> Update status

Screen Commands: (start screen session as root so someone else can pick it up)

% screen	start screen session
% screen -ls	list the screen sessions
CTRL-a d	detach screen
% screen -r	attach screen
% screen -r pid.tty.hostname	attach specific screen session (if you have more than one open)

Define Console

Local> prompt
 Type show serv
 Type connect wdpcm1

Username: sas
 Password: sas

Type ccon <conn_name>

The point-of-contact for Tru64 servers will tell you the connection name and network interface to use for each system. Write the information below on the white board for reference.

	Connection	Network Interface
dreos	_____	_____

dlapis _____
drgarnet _____
drzinc _____

Build and Restore Root

Check that machine is halted.
Verify CDROM drive has the OS CD marked as:

“Compaq Tru64 UNIX Version 5.1B Operating System Volume 1”

1) Boot CD-ROM.

☐ _____ initial

Get device information on boot disk and cdrom

>>> show dev

>>> show config

Boot disk (e.g. DKA0)

CD-ROM device (e.g. DKA400)

Set BOOTDEF_DEV to null

>>> set bootdef_dev ""

Set BOOTDEF_DEV to null string to prevent the installation process from copying the hardware configuration from the root system.

Boot CDROM

>>> boot -fl A DKA400

On a graphics console:

English Installation window, click **OK**

Installation Welcome window, click **File** then **Quit**

On serial console:

- 1) U.S. English Installation
- 2) Installation with Worldwide Language Support
- 3) Exit Installation

Enter your choice: **3**

Enter 3 to exit installation to Unix Shell.

2) Create boot disk.

☐ _____ initial

TERM=vt100; export TERM

Show system devices to get boot disk drive (e.g. dsk0)

hwmgr -v dev

Run “disklabel -r” on each available disk. Pick the 18GB disk as the boot disk and leave the larger size disk for the application data.

This document is using 'dsk0' as an example for the boot disk.

Write boot disk configuration to a temporary file

```
# disklabel -rw -t advfs dsk0
# disklabel -r dsk0 > /tmp/label-dsk0
```

Edit the disk configuration

```
# vi /tmp/label-dsk0
- Modify the disk partition according to requirements
  (see below for the proposed 18GB disk layout)
- Verify fstype for partition b is “swap”
- Verify fstype for other partitions are “unused”
- Do not include comma (,) in the number partitions
- Verify the disk space allocation for each partition
  The partition size is in 512K (400,000 = ~200MB)
  The offset starts at 0; next offset = offset + size
```

Proposed 18GB boot disk layout for dreos, drzinc, drgarnet, and drlapis:

Partition	Size	Offset	~ Size
a	600,000	0	300MB (root)
b	8,000,000	600,000	4.0GB (swap)
c	35,547,048	0	18.0GB
d	5,000,000	8,600,000	2.5GB (/usr)
e	5,000,000	13,600,000	2.5GB (/var)
f	4,000,000	18,600,000	2.0GB (/tmp)
g	6,000,000	22,600,000	3.0GB (/usr/local)
h	<n>	28,600,000	3.3GB (/usr/users)

where <n> = c (size) – h (offset)
(Ex: if c=35,547,048, then <n>=6,947,048)

Create boot disk with the new disk configuration

```
# disklabel -R -r -t advfs dsk0 /tmp/label-dsk0 dsk0    (create boot disk)
# disklabel -r dsk0                                     (verify partitions and sized)
```

☐ Verify the boot disk (e.g. **dsk0**) partition with the sizes specify above

3) Create root domain.

☐ _____ initial

```
# mkdir /var/root
# mkfdmn /dev/disk/dsk0a root_dom
# mkfset root_dom root
# mount root_dom#root /var/root
```

4) Create tape device.

☐ _____ initial

```
# /sbin/dn_setup -install_tape
```

Call SunGard point-of-contact to load the OS tape

Get the tape device

```
# hwmgr -v d
```

This document is using "tape0_d1" as an example for the tape device.

Verify the tape is in the drive

```
# mt -f /dev/ntape/tape0_d1 status
```

5) Restore root partition.

☐ _____ initial

```
# vrestore -x -o no -f /dev/ntape/tape0_d1 -D /var/root
```

6) Clear old hardware devices.

☐ _____ initial

o Execute script /var/root/etc/dr/**dr.os_deldev**

The hardware files are saved in /var/root/Olddev. Verify old hardware files are removed:

```
# cd /var/root/etc
# ls dec* ddc*d* dcd* dfsc*
# cd ../cluster/members/member
# ls .Booted etc/cfginfo etc/dfsl*
# cd /var/root/dev
# ls disk rdisk cport tape ntape
```

☐ Verify old devices are removed

(OR)

o Manually remove the old restored devices

Remove old hardware devices to Olddev directory

```
# cd /var/root/etc
# rm dec* dcd* dcd* dfsc*
# cd /var/root/cluster/members/member
# rm -fr .Booted etc/cfginfo etc/dfsl*
```

Remove old disk and cport config

```
# cd /var/root/dev
# rm disk/* rdisk/* cport/* tape/* ntape/*
```

7) Change hostname, IP, netmasks, etc.

☐ _____ initial

Execute script /var/root/etc/dr/**dr.os_cpsysfiles**

And modify the following files in /var/root/etc:

```
# ifconfig -a          (to get network interface)
# vi sysconfigtab      (search for swap, e.g. swapdevice=/dev/dsk/dsk0b)
# vi rc.config          (Update network interface, e.g. NETDEV_0="tu2")
```

```
# grep NR rc.config      (Verify all netrain configurations are removed)
# grep CONFIG rc.config  (Verify network configurations)
```

drzinc:

```
# vi inet.local    (Update network interface, e.g. lan_config -i tu0 -a 0 -s 100 -x 1)
```

For manual instructions, see “**Network Setup**” in MANUAL INSTRUCTIONS section at the end of this document.

8) Disable start/stop scripts that will not be started at D/R site.

☐ _____ initial

Execute script /var/root/etc/dr/**dr.os_rcdrename**

For manual instructions, see “**Start/Stop rc scripts**” in MANUAL INSTRUCTIONS section at the end of this section.

Build and Restore Boot Disk

Restore other partitions (in order of /usr, /var, /usr/local, /usr/users)

1) Create domains and filesets.

☐ _____ initial

Execute script below to create the required file domains and filesets; mount all files system.

```
# /var/root/etc/dr/dr.os_mkfdmn dsk0  (18GB disk configuration)
# df -k                                (verify all files system are mounted)
```

For manual instructions, see “**Boot Disk Configuration**” in *Manual Instructions* section at the end of this section.

☐ Setup the links in /var/root/etc/fdmns directory.

☐ _____ initial

Execute script below to set up links for the system boot disk

```
# /var/root/etc/dr/dr.os_fdmns dsk0  (for 18 GB disk configurations)
# ls -l /var/root/etc/fdmns/*         (verify fdmns links)
```

For manual instructions, see “**Fdmns Links Setup**” in *Manual Instructions* section at the end of this section.

2) Restore the partitions (in order of /usr, /var, /usr/local, /usr/users)

☐ _____ initial

Tape should already be in position for restore, if not do the following:

```
# mt -f /dev/ntape/tape0_d1 rewind
# mt -f /dev/ntape/tape0_d1 fsf 1
```

dreos: (only)

☐ _____ initial

Execute the following scripts:

```
% cd /var/root/etc/dr
# ./dr.res_usr tape0_d1
# more /var/usr/local/usr.restore
```

☐ Verify the /usr is restored correctly

```
# ./dr.res_var tape0_d1
# more /var/usr/local/var.restore
```

☐ Verify the /var is restored correctly

/usr/local is too big to restore all the data, only restore the necessary directories:

```
# cd /var/usr/local
# vrestore -i -f /dev/ntape/tape0_d1
(/) ls
(/) add lib dr bin etc sbin include oracle
(/) extract
```

☐ Verify the /usr/local is restored correctly

drgarnet/drlapis/drzinc: (only)

☐ _____ initial

Execute the following scripts:

```
% cd /var/root/etc/dr
# ./dr.res_usr tape0_d1
# more /var/usr/local/usr.restore
```

☐ Verify the /usr is restored correctly

```
# ./dr.res_var tape0_d1
# more /var/usr/local/var.restore
```

☐ Verify the /var is restored correctly

```
# ./dr.res_local tape0_d1
# more /var/usr/local/var.restore
```

☐ Verify the /usr/local is restored correctly

dreos/drlapis/drzinc: (only)

☐ _____ initial

```
# ./dr.res_home tape0_d1
# more /var/usr/local/home.restore
```

- ☐ Verify user's home directories are restored correctly

Notes: On *dreos* and *drgarnet*, restoring only admins and dbas accounts to /home directory.

(OR)

Manually type in the restore commands as follows – only if the scripts above don't run:

```
# date; vrestore -xv -o no -f -D /var/usr > /var/usr/local/usr.restore
# date; vrestore -xv -o no -f /dev/ntape/tape0_d1 -D /var/var > /var/usr/local/var.restore
# date; vrestore -xv -o no -f /dev/ntape/tape0_d1 -D /var/usr/local > /var/usr/local/local.restore
```

drlapis/drzinc: (only)

```
# date; vrestore -xv -o no -f /dev/ntape/tape0_d1 -D /var/usr/users >
/var/usr/local/home.restore
```

dreos: (only)

```
# date; vrestore -xv -o no -f /dev/ntape/tape0_d1 -D /var/home> /var/usr/local/home.restore
```

NOTES:

If a partition you are restoring is too big for the configured size, use **-i** (interactive) restore option to select the directories you wish to restore.

```
# vrestore -i -f /dev/ntape/tape0_d1
restore> select <dir1>
restore> select <dir2>
restore> extract
```

3) Halt the system

- ☐ _____ initial

halt

BOOT

1) Boot the system up with generic kernel.

- ☐ _____ initial

```
>>> show dev (to get boot disk device, e.g. dka0)
```

```
>>> boot -fl s -fi genvmunix DKA0
```

```
# TERM=vt100; export TERM
```

Once booted to generic kernel, add swap and build new kernel.

a. Create devices and mount all files system

```
# /sbin/mountroot (Create all the devices)
# /sbin/bcheckrc (Mount all files system in /etc/fstab)
# df -k (Verify all files system in /etc/fstab are mounted including /tmp)
```

b. Set file permission for /tmp directory

```
# chmod 1777 /tmp
```

c. Add swap

```
# swapon -s                (Display swap space utilization)
# swapon -a /dev/disk/dsk0b (Add swap partition if no swap space shown)
# vi /etc/sysconfigtab
    Verify swapdevice has the correct swap partition.
```

d. Build a new kernel and move it to the root directory

```
# doconfig
```

```
Enter <HOSTNAME> for the name of configuration file (e.g. DREOS)
Enter Y to confirmation prompt
Press RETURN to continue displaying ***KERNEL OPTION SELECTION***
Enter a number that has option "all of the above" at the Kernel build question
Enter Y to confirmation message
Enter N to edit configuration
```

The new kernel is /sys/<HOSTNAME>/vmunix, copy to / (root) directory

```
# cp -p /vmunix /vmunix.old
# mv /sys/<HOSTNAME>/vmunix /vmunix
```

e. Halt the system

```
# halt
```

2) Boot with the new kernel.

☐ _____ initial

a. Change boot definition

```
>>> show auto_*
>>> set auto_action BOOT

>>> show dev (to get the boot disk device, e.g. DKA0)
>>> show boot*
>>> set boot_osflags a
>>> set bootdef_dev DKA0
```

b. Boot to single user mode

```
>>> boot -fl s

# /sbin/bcheckrc (to mount all files system)
# TERM=vt100; export TERM
```

Verify *fstab*, *hosts*, *rc.config*, *inet.local*, *routes*, *sysconfigtab* in **/etc** directory before booting to multi-user mode.

c. Boot to multi-user mode

```
# exit
```

3) Disable crontabs.

☐ _____ initial

```
# cd /var/spool/cron/crontabs
# mkdir crontabs.hold
# mv * crontabs.hold
# /sbin/init.d/cron stop
# sudo /sbin/init.d/cron start
```

```
# ls /var/spool/cron/atjobs/*
# rm /var/spool/cron/atjobs/*
```

4) Fix CPU license number.

☐ _____ initial

drgarnet/drlapis/drzinc: (only)

On **drlapis** and **drgarnet**, and maybe **drzinc** you will get an error message of ‘too many users already login’ when you login with your username. This was due to the number of CPU license is not large enough for the current restored system.

7/03 – There was not enough CPU license number in the license file.

Do the following to correct the CPU licenses:

Login as root.

lmf

lmf> list

Below is the license listing on lapis:

Product	Status	Users: Total	Active
DECEVENT	terminated		
ADVFS-UTILITIES	active	unlimited	
SYSV	active	unlimited	
OSF-DEV	active	unlimited	
OSF-BASE	active	unlimited	
OSF-BASE	active, multiple	unlimited	
OSF-SVR	active	unlimited	
OSF-USR	active	unlimited	
OSF-USR	active, multiple	unlimited	
ASE-OA	active	unlimited	

Change the value in “**Number of units:**” to 2700 for each of the license listed above. For license that have multiple entries, such as OSF-BASE and OSF-SVR, you need to specify the “**Authorization Number:**” with the modify command.

lmf> modify ADVFS-UTILITIES

lmf> modify SYSV

lmf> list full for OSF-BASE (to get the Authorization Number)

lmf> modify OSF-BASE DEC ALS-NQ-1999MAR30-1141

```
lmf> modify OSF-BASE DEC ALS-NQ-1999MAR30-1150
lmf> modify OSF-SRV
lmf> list full for OSF-USR
lmf> list modify OSF-USR DEC ALS-NQ-1999MAR30-1147
lmf> modify ASE-OA
```

```
lmf> reset
lmf> exit
```

If one of the multiple license (such as OSF-BASE) having problem saving the Number of Units, then try to disable one of them:

Example:

```
lmf> disable OSF-BASE DEC ALS-NQ-1999MAR30-1150
```

Log off as root.

5) Verify network.

☐ _____ initial

```
% ifconfig -a
% /usr/sbin/netstat -i
% netstat -nr
```

Verify you have network connectivity to NIH and outside.

6) Verify date and time.

☐ _____ initial

```
# date
```

If date is not correct, change it:

```
# date mmddyy
(e.g. date 120815052003 = 12/8/2003 3:05pm)
```

7) Verify ACL is enabled on lapis and garnet.

☐ _____ initial

drgarnet/drlapis: (only)

```
% sysconfig -q sec
% grep acl /etc/sysconfigtab
```

8) Create nbsproj account.

☐ _____ initial

drzinc: (only)

```
# /usr/sbin/groupadd -g 1331 nbsproj
# /usr/sbin/groupadd -g 1859 iappprod
# /usr/sbin/useradd -c "nbsproj owner" -d /usr/users/nbsproj -g nbsproj -m -s /bin/ksh -u 30542 \
```

```
nbsproj
# /usr/sbin/useradd -c "iappprod owner" -d /usr/users/iappprod -g iappprod -m -s /bin/ksh -u \
29883 iappprod
# passwd nbsproj
# passwd iappprod
```

9) Notify Adrienne that the system is up and ready for application restores.

☐ _____ initial

Prepare for Application Restores

1) Find the available disk(s).

☐ _____ initial

```
# hwmgr -v dev (e.g. dsk1)
# disklabel -rw -t advfs dsk1
```

2) Create file domain for the applications.

☐ _____ initial

Create one big domain for all the filesets. Use addvol if necessary.

```
# mkfdmn /dev/disk/dsk1c dr_dom
```

dreos (application-prep):

1) Create fileset for /usr/users and /scratch.

☐ _____ initial

```
# /etc/dr/dr.app_mkfsuser dr_dom
```

2) Restore dba home directories.

☐ _____ initial

```
# /usr/local/dr/siduser.dr -x -s drlocal -d /usr/local/dr
```

Extract files from /usr/local/dr/drlocal/appl/drlocal.ufiles.tar.gz
Creates home directory if it does not exist

Verify owner:group in /usr/users directory
ls -l /usr/users

If owner:group are incorrect, run script:
/etc/dr/dr.app_fxdrlocal
ls -l /usr/users (to verify owner:group are correct)

3) Create application filesets.

☐ _____ initial

```
# /etc/dr/dr.app_mkfs dr_dom
```

The script:

creates and mounts the following filesets:

```
afpsp, afpspbin, pacf, pacfbin, acf_oracle (/apps/acf), crispprd, crispprdbin,
nihdirp2, nihdirp2bin, dumps, backups, export, oramaint
```

7/05 test : does not include nihdir (**nihdirp2** and **nihdirp2bin**)

creates the following directories for ACF printing:

```
/apps/acf/gates_print
/apps/acf/gates_print.invalid
```

more /etc/fstab (verify application domain name)

4) Create dumps and backups directory.

☐ _____ initial

```
# /etc/dr/dr.app_dumpd
```

The script above creates the following directories:

```
/dumps/afpsp and /backups/afpsp/appl
/dumps/pacf and /backups/pacf/appl
/dumps/crispprd and /backups/crispprd/appl
/dumps/gmp and /dumps/gmp/appl
/dumps/gmpub and /dumps/gmpub/appl
/dumps/nihdirp2 and /backups/nihdirp2/appl
/export/[log,dmp,sql,crontablog]
```

12/05 test : does not include *nihdir* (/dumps/nihdirp2, /backups/nihdirp2/app)

12/05 test: test does not include crispprd, but directories are created.

drgarnet (application-prep):

1) Create fileset for /usr/users.

☐ _____ initial

```
# sudo /etc/dr/dr.app_mkfsuser dr_dom
```

2) Restore admin and dba home directories.

☐ _____ initial

```
# sudo /usr/local/dr/siduser.dr -x -s drlocal -d /usr/local/dr
```

Extract files from /usr/local/dr/drlocal/appl/drlocal.ufiles.tar.gz
Creates home directory if it does not exist

Verify owner:group in /usr/users directory

```
# ls -l /usr/users
```

If the owner:group are incorrect, run script:

```
# /etc/dr/dr.fxdrlocal
```

```
# ls -l /usr/users (to verify owner;group are correct)
```

- ☐ _____ Verify owner and group are correct

3) Create application filesets.

- ☐ _____ initial

/etc/dr/**dr.app_mkfs** dr_dom

The script:

creates and mounts the following filesets:

oracle, orabin, plsqr for pmsprod

creates the following directories:

/backups

/dumps

/apps/pms-hold

more /etc/fstab (verify application domain name and all needed filesets are mounted)

- ☐ _____ Verify mount points exist and in /etc/vfstab file

drlapis (application-prep):

1) Create application filesets.

- ☐ _____ initial

/etc/dr/**dr.app_mkfs** dr_dom

The script creates and mounts the following filesets: oas, pmspoas, pmspoasbin, backups.

more /etc/fstab (verify application domain name)

- ☐ _____ Verify mount points exist and in /etc/vfstab file

drzinc (application-prep):

1) Create application filesets.

- ☐ _____ initial

/etc/dr/**dr.app_mkfs** dr_dom

The script above creates and mount the following filesets:

igelpod, g816prod, iaappod, backups

more /etc/fstab (verify application domain name)

Application Setup

1) Create application filesets.

Login as your username.

- ☐ _____ initial

Login using your username to verify that it is working.

4) Modify sudoers file.

☐ _____ initial

drzinc: (only)

% sudo visudo

Go to the bottom of the file and uncomment all the lines below "Uncomment for DR 7/07"

4) Modify hosts.allow file.

☐ _____ initial

drzinc: (only)

% sudo vi /etc/hosts.allow

Go to the bottom of the file and uncomment all the lines below "Uncomment for DR 7/07"

4) Configure and startup Connect:Direct.

☐ _____ initial

eos Connect:Direct version 3.4.01

garnet Connect:Direct version 3.5

dreos/drgarnet: (only)

- Execute script to install license key and net map configuration files

% sudo etc/dr/**dr.cd_config**

For manual instructions, see "**Connect:Direct Setup**" in MANUAL INSTRUCTIONS at the end of this document.

- Startup Connect:Direct

% sudo **/sbin/init.d/conn_dir start**

% ps -ef | grep conn_dir

- Verify Connect:Direct is running.

% sudo **su - stem**

% cd /usr/opt/conn_dir/ndm/bin

% **direct**

direct> submit file=sample.cd;

direct> quit;

Verify file "cddelete.me" in stem's \$HOME directory.

Application Restores

You can login as root or use sudo with your account to restore the applications.

While the application restore are running, mirror the local boot disk to the disk on the SAN. This is for in case the local boot disk has problem as it did in previous test. Mirror the boot disk by using **rsync**.

☐ _____ initial

% sudo hwmgr -v d (to find the 18GB SAN disk)

% sudo **disklabel -r dsk0 > /tmp/label-dsk0**

% sudo vi /tmp/label-dsk0

Change the /dev/rdisk/dsk to point the san disk, also change the “type” and “disk” – the information retrieved from “hwmgr -v d”

Create the boot disk on the SAN disk using the same disk configuration as the local disk

% sudo **disklabel -R -r -t advfs dsk0 /tmp/label-dsk0 <san disk>**

% sudo **disklabel -r <san disk>**

Create the mirror boot disk directory

% sudo mkdir /bkroot /bkusr /bkvar /bklocal /bkusers

Modify fstab to add mirror boot disk directory

% cd /etc

% sudo cp fstab fstab.<yyyymmdd>

% sudo vi fstab

Add in all the mount points for /bk* directories

Mount the /bk* directories

% sudo mount /bkroot

% sudo mount /bkusr

....

Run rsync script

% sudo /usr/local/etc/rsync.system.disk

dreos (application-restore):

Update DR Web Page status with onsite DR coordinator. Suggested text “DREOS application files are being restored”.

Get the name of the tape drive and write the information below on the white board for reference.

Tape drives:

/dev/tape/_____

/dev/tape/_____

/dev/tape/_____

Pacf (on eos):

1) Restore vdump from tape

☐ _____ initial

Request tape “**eos pacfdrbkup.**” This will span to multiple tapes. It will request the second tape “**eos pacfdrbkup2.**” Note the times tapes are requested.

/usr/local/dr/vdmprst.scr -d /dev/ntape/tape#_d1 -s pacf

Restores files:

/dumps/pacf/clone_ora*_acf_pacf.vdump.*
/backups/pacf/appl/pacf.ufiles.tar.gz

7/06: data expanded to 3 tapes; data was not restored correctly – user ended up testing testing on silver

Tape 1 Start:_____ End: _____
Tape 2 Start:_____ End: _____
Tape 3 Start:_____ End: _____

2) Restore user files and other requested files (ran about 1:15 7/04)

☐ _____ initial

% sudo /usr/local/dr/**siduser.dr -x -s** pacf

The script above extract files from /backups/pacf/appl/pacf.ufiles.tar.gz.

Verify owner:group in /usr/users directory
ls -l /usr/users

If owner:group are incorrect, run script:
/etc/dr/**dr.acct_fxpacf**
ls -l /usr/users (to verify owner:group are correct)

3) Run vrestore for /orabin and /oracle backups. The vdmrestore command will uncompress the vdump file and then run vrestore. Do the /orabin first since it will finish faster, and once it starts the vrestore process the vdmrestore command can be started for the /oracle data – the /orabin files will be vrestored before the uncompress finishes for the /oracle data. There will be some disk contention, but it should still be faster than a single task at a time. If the tape dump is finished early enough (before 6?), then run one command at a time for the better performance.

☐ _____ initial

ls /dumps/pacf

/usr/local/dr/**vdmrestore **
/dumps/pacf/clone_orabin_acf_pacf.dump.HHMM.DATE.gz /orabin/acf/pacf/

/usr/local/dr/**vdmrestore **
/dumps/pacf/clone_oracle_acf_pacf.dump.HHMM.DATE.gz /oracle/acf/pacf

4) Verify ownership.

☐ _____ initial

<u>Directory</u>	<u>Owner:Group</u>
/oracle/acf/pacf	pacf:pacf
/orabin/acf/pacf	pacf:pacf

5) Notify DBAs when restore is complete so they can start the database and update the DR web page that the database is available.

☐ _____ initial

Afsp (on eos):

1) Restore vdump files from tape

☐ _____ initial

Request tape "eos afpsdrbkup."

/usr/local/dr/vdmprest.scr -d /dev/ntape/tape#_d1 -s afps

Tape 1 Start:_____ End: _____

Restores files:

/dumps/afps/clone_ora*_dfo-afps_afps.dump.*

/backups/afps/appl/afps.ufs.tar.gz

7/06: ~30 minutes to complete

2) Restore user files and other requested files

☐ _____ initial

/usr/local/dr/siduser.dr -x -s afps

Verify owner:group in /usr/users directory

ls -l /usr/users

If owner:group are incorrect, run script:

/etc/dr/dr.acct_fxafps

ls -l /usr/users (to verify owner:group are correct)

3) Run vrestore for /orabin and /oracle backups. The vdmprestore command will uncompress the vdump file and then run vrestore. Note times restores started/finished.

☐ _____ initial

ls /dumps/afps

/usr/local/dr/vdmprestore \

/dumps/afps/clone_oracle_dfo-afps_afps.dump.HHMM.DATE.gz /oracle/dfo-afps/afps/

7/06: ~30 minutes to complete

/usr/local/dr/vdmprestore \

/dumps/afps/clone_orabin_dfo-afps_afps.dump.HHMM.DATE.gz /orabin/dfo-afps/afps/

7/06: ~25 minutes to complete

4) Verify ownership.

☐ _____ initial

Directory

/oracle/dfo-afps/afps

/orabin/dfo-afps/afps

Owner:Group

afps:afps

afps:afps

- 5) Notify DBAs when restore is complete so they can start the database and update the DR web page that the database is available.

☐ _____ initial

Crispprd (on eos):

- 1) Restore vdump files from tape

☐ _____ initial

Request tape “**eos crisprdbkup.**” This will span to two tapes. It will request the second tape “**eos crisprdbkup2.**” Note the times tapes are requested.

```
# /usr/local/dr/vdmprst.scr -d /dev/ntape/tape#_d1 -s crispprd
```

Tape 1 Start: _____ End: _____

Tape 2 Start: _____ End: _____

Restores files:

/dumps/crispprd/clone_ora*_oer-commons_crispprd.dump.*

/backups/crispprd/appl/crispprd.ufiles.tar.gz

7/06: ~1 hours 50 minutes to complete (tape1 - ~1 hour 10 minutes; tape2 - ~40 minutes)

- 2) Restore user files and other requested files

☐ _____ initial

```
# /usr/local/dr/siduser.dr -x -s crispprd
```

Verify owner:group in /usr/users directory

```
# ls -l /usr/users
```

If owner:group are incorrect, run script:

```
# /etc/dr/dr.acct_fxcrisp
```

```
# ls -l /usr/users (to verify owner:group are correct)
```

- 3) Run vrestore for /orabin and /oracle backups. The vdmprestore command will uncompress the vdump file and then run vrestore. Note times restores started/finished.

☐ _____ initial

```
# ls /dumps/crispprd
```

```
# /usr/local/dr/vdmprestore \
```

```
/dumps/crispprd/clone_oracle_oer-commons_crispprd.dump.HHMM.DATE.gz \
```

```
/oracle/oer-commons/crispprd/
```

7/06: ~2 hours 10 minutes to complete

☐ _____ Verify data in *oracle/oer-commons/crispprd*

```
# /usr/local/dr/vdmprestore \
```

```
/dumps/crispprd/clone_orabin_oer-commons_crispprd.dump.HHMM.DATE.gz \
/orabin/oer-commons/crispprd/
```

7/06: ~10 minutes to complete

☐ _____ Verify data in /orabin/oer-commons/crispprd

4) Verify ownership.

☐ _____ initial

<u>Directory</u>	<u>Owner:Group</u>
/oracle/oer-commons/crispprd	crispprd:crispprd
/orabin/oer-commons/crispprd	crispprd:crispprd

5) Notify DBAs when restore is complete so they can start the database and update the DR web page that the database is available.

☐ _____ initial

Nihdirp2 (on eos):

1) Restore vdump files from tape

_____ initial

Request tape "eos nihdrbkup."

/usr/local/dr/vdmprest.scr -d /dev/ntape/tape#_d1 -s nihdirp2

Tape 1 Start: _____ End: _____
Tape 2 Start: _____ End: _____

Restores files:
/dumps/nihdirp2/clone_ora*_cit-nihdir_nihdirp2.vdump.*
/backups/nihdirp2/appl/nihdirp2.ufiles.tar.gz

Verify data /dumps/nihdirp2 and /backups/nihdirp2/appl

2) Restore user files and other requested files

_____ initial

/usr/local/dr/siduser.dr -x -s nihdirp2

Verify owner:group in /usr/users directory
ls -l /usr/users

If owner:group are incorrect, run script:
/etc/dr/dr.acct_fxnihdirp2
ls -l /usr/users (to verify owner:group are correct)

3) Run vrestore for /orabin and /oracle backups. The vdmprestore command will uncompress the vdump file and then run vrestore. Note times restores started/finished.

_____ initial

ls /dumps/nihdirp2

```
# /usr/local/dr/vdmprestore \  
  /dumps/nihdirp2/clone_oracle_cit-nihdir_nihdirp2.dump.HHMM.DATE.gz \  
  /oracle/cit-nihdir/nihdirp2/
```

_____ Verify data in /oracle/cit-nihdir/nihdirp2

```
# /usr/local/dr/vdmprestore \  
  /dumps/nihdirp2/clone_orabin_cit-nihdir_nihdirp2.dump.HHMM.DATE.gz \  
  /orabin/cit-nihdir/nihdirp2
```

_____ Verify data in /orabin/cit-nihdir/nihdirp2

4) Verify ownership. of and

_____ initial

Directory	Owner:Group
/oracle/cit-nihdir/nihdirp2	nihdirp2:nihdirp2
/orabin/ cit-nihdir/nihdirp2	nihdirp2:nihdirp2

- 5) Notify DBAs when restore is complete so they can start the database and update the DR web page that the database is available.

gmp,gmpub (on eos):

1) Create filesets.

☐ _____ initial

/etc/dr/dr.app_mkfs_gmp

2) restore vdump files from tape

☐ _____ initial

request tape "eos gmpdrbkup".

/usr/local/dr/vdmprst.scr -d /dev/ntape/tape#_d1 -s gmp

Tape 1 Start:_____ End: _____
Tape 2 Start:_____ End: _____

Restores files:

```
/dumps/gmp/*  
/backups/gmp/appl/*  
/dumps/gmpub/*  
/backups/gmpub/appl/*
```

7/05: ~2 hours 10 minutes to complete

3) Restore user files and other requested files

☐ _____ initial

```
# /usr/local/dr/siduser.dr -x -s gmp
# /usr/local/dr/siduser.dr -x -s gmpub
```

Verify owner:group in /usr/users directory
ls -l /usr/users

If owner:group are incorrect, run script:
/etc/dr/**dr.acct_fxgmp**
ls -l /usr/users (to verify owner:group are correct)

4) Run vrestore for /orabin /and /oracle backups. Note times restores started/finished.

☐ _____ initial

```
# /usr/local/dr/vdmprestore \
  /dumps/gmp/clone_oracle_nigms-irmb_gmp.vdump.HHMM.DATE.gz \
  /oracle/nigms-irmb/gmp
```

☐ _____ Verify data in /oracle/nigms-irmb/gmp

```
# /usr/local/dr/vdmprestore \
  /dumps/gmp/clone_orabin_nigms-irmb_gmp.vdump.HHMM.DATE.gz \
  /orabin/nigms-irmb/gmp
```

☐ _____ Verify data in /orabin/nigms-irmb/gmp

```
# /usr/local/dr/vdmprestore \
  /dumps/gmpub/clone_oracle_nigms-irmb_gmpub.vdump.HHMM.DATE.gz \
  /oracle/nigms-irmb/gmpub
```

☐ _____ Verify data in /oracle/nigms-irmb/gmpub

```
# /usr/local/dr/vdmprestore \
  /dumps/gmpub/clone_orabin_nigms-irmb_gmpub.vdump.HHMM.DATE.gz \
  /orabin/nigms-irmb/gmpub
```

☐ _____ Verify data in /orabin/nigms-irmb/gmpub

5) Verify ownership.

☐ _____ initial

<u>Directory</u>	<u>Owner:Group</u>
/oracle/nigms-irmb/gmp	gmp:gmp
/orabin/nigms-irmb/gmp	gmp:gmp
/oracle/nigms-irmb/gmpub	gmpub:gmpub
/orabin/nigms-irmb/gmpub	gmpub:gmpub

6) Notify DBAs when restore is complete so they can start the database.

☐ _____ initial

General eos

- 1) Remove things from /dumps and /backups when databases are restored to free up space for exports
- 2) Note final “df -k”
- 3) Once all databases are ready, or Tuesday am, update D/R web page status with onsite NIH D/R coordinator. Suggested text: “DREOS available for testing”
- 4) Check performance stats during testing; memory, load, swap

TIMING NOTES

<u>Instance</u>	<u>siduser.dr</u>	<u>vdmprestore times</u>		<u>verify</u>	<u>notify</u>
	<u>Time</u>	<u>orabin</u>	<u>oracle</u>	<u>owners</u>	<u>DSB</u>
afpsp	_____	_____	_____	_____	_____
pacf	_____	_____	_____	_____	_____
nihdrp2	_____	_____	_____	_____	_____
gmp	_____	_____	_____	_____	_____
gmpub	_____	_____	_____	_____	_____

drgarnet (application-restore):

Update the DR Web Page Status with the onsite NIH/DR coordinator. Suggested text: “PMS DR application files are being restored”

Get the name of the tape drive and write the information below on the white board for reference.

Tape Drives: _____

- 1) Request tape “**garnet pmsdrbkup**”. The backup may span multiple tapes, once the first is done, request “garnet pmsdrbkup 2”.

☐ _____ initial

- 2) Restore vdump files from tape (approx 3 hours)

☐ _____ initial

/usr/local/dr/**vdmprst.scr -d /dev/ntape/tape#_d1 -s pmsprod**

The command above restores the following files:

/dumps/pmsprod/clone_ora*_dpm-pms_pmsprod.dump.*
/backups/pmsprod/appl/pmsprod.ufiles.tar.gz

7/06: ~3 hour 35 minutes to complete (tape1 - ~3 hours; tape2 - ~35 minutes)

☐ Verify data in `/dumps/pmsprod` and `/backups/pmsprod/appl`

- 3) Run `vrestore` for `/oracle` and `/orabin` backups. (uncompresses `vdump` file, issues `vrestore` command to restore files to appropriate directory.) Note times restores started/finished. (Approx 10 min for `/orabin` directory and 2+ hours for `/oracle` directory)

☐ _____ initial

`ls /dumps/pmsprod`

```
# /usr/local/dr/vdmprestore \  
  /dumps/pmsprod/clone_oracle_dpm-pms_pmsprod.dump.HHMM.DATE.gz \  
  /oracle/dpm-pms/pmsprod/
```

7/06: ~1 hour to complete

☐ _____ Verify data in `/oracle/dmp-pms/pmsprod`

```
# /usr/local/dr/vdmprestore \  
  /dumps/pmsprod/clone_orabin_dpm-pms_pmsprod.dump.HHMM.DATE.gz \  
  /orabin/dpm-pms/pmsprod/
```

7/06: ~20 minutes to complete

☐ _____ Verify data in `/orabin/dmp-pms/pmsprod`

- 4) Check the ACLs on `/oracle/dpm-pms/pmsprod/plsql`

☐ _____ initial

The ACL should be

```
# file: /oracle/dpm-pms/pmsprod/plsql  
# owner: pmsbatch  
# group: pmsread  
#  
user::rwx  
group:---  
group:pmsread:r-x  
group:pms:rwx  
other:---
```

```
# getacl /oracle/dpm-pms/pmsprod/plsql  
Fix if not correct – run /usr/local/dr/setacl.dr  
# /usr/local/dr/setacl.dr
```

- 5) Create the needed `/usr/users/` files by running

☐ _____ initial

```
# /usr/local/dr/siduser.dr -x -s pmsprod
```

```
Verify owner:group in /usr/users directory  
# ls -l /usr/users
```

If owner:group are incorrect, run script:
 # /etc/dr/dr.acct_fxgmp
 # ls -l /usr/users (to verify owner:group are correct)

6) Reboot the system.

☐ _____ initial

7) Notify DBAs when restore is complete so they can start the database and update the DR web page that the database is available.

☐ _____ initial

TIMING NOTES

=====					
Instance	ddrestore time	vdmprestore orabin	times oracle	verify owners	notify DSB
pmsprod	_____	_____	_____	_____	_____

drlapis (application-restore):

☐ _____ initial

- 1) The applications need to be restored are on the same tape as the system backup tape. List of filesets included on lapis tape (in order): /, /usr, /usr/var, /usr/local, /usr/users, /backups/OAS/pmspoas, /oramaint/orasoft/OAS/, /orabin/dpm-pms/pmspoas

```
# mt -f /dev/ntape/tape0_d1 rewind
# mt -f /dev/ntape/tape0_d1 fsf 5
```

Run the following scripts:

```
# cd /etc/dr
# ./dr.res_oas tape0_d1
# ./dr.res_oramaint tape0_d1
# ./dr.res_binoas tape0_d1
```

(OR)

Manually type in the restore commands as follows:

```
# cp /etc/dr/scripts/* /oramaint/scripts
# cd /backups/OAS/pmspoas
# vrestore -vx -o no -f /dev/ntape/tape0_d1 -D /backups/OAS/pmspoas
# vrestore -vx -o no -f /dev/ntape/tape0_d1 -D /oramaint/orasoft/OAS
# vrestore -vx -o no -f /dev/ntape/tape0_d1 -D /orabin/dpm-pms/pmspoas
```

7/05: ~3 hours to complete – it took much longer than previous times

- 2) Once the files are restored from tape, the /oracle/dpm-pms/pmspoas directory needs to be untarred from /backups/OAS/pmspoas

Run the following scripts:

```
# cd /usr/local/dr
# ./pmsuntar
```

(OR)

Manually type in the restore commands as follows:

```
Determine newest file in /backups/OAS/pmspoas/application directory
# cd /
# /usr/local/bin/tar -xzf /backups/OAS/pmspoas/application/pmspoas.DOW.tar.gz
  (with DOW replaced by the appropriate day of the week to indicate the newest file)
# mkdir -p /oracle/dpm-pms/pmspoas/Apache/Apache/logs
```

*The pmspoas binaries took about an hour to restore from tape. The others are small and took a few seconds.

- 3) Reboot the system after the application restore is completed
- 4) Notify the DBAs when restore is complete so they can complete the OAS restore and update the DR web page that the OAS is available.
- 5) Once all databases are ready, or Tuesday AM, update DR web page status with onsite NIH DR coordinator. Suggested text: "DRGARNET and DRLAPIS are available for testing".

TIMING NOTES

```
=====
                                start                                end
=====
```

```
pmspoas :backups
pmspoas: oramaint
pmspoas: orabin
```

```
=====
```

drzinc (application-restore):

- 1) Update DR Web Page status with onsite DR coordinator. Suggested text "NBS DR application files are being restored.

☐ _____ initial

- 2) Note names of tape drives.

☐ _____ initial

Write the information below on the white board for reference.

DAT72: /dev/tape/_____

- 3) Start a script session to capture commands/output.

☐ _____ initial

- 4) Request tape “**zinc nbsdrbkup**” in dat72 drive. This will restore data from halite and zinc.

☐ _____ initial

Run **/usr/local/dr/vdmprst.scr** to get the data off the tape.

/usr/local/dr/vdmprst.scr -d /dev/ntape/tape#_d1 -s g816prod

This will restore:

- o /oraappl/od-nbs/backups/drcold/
- o /oraappl/od-nbs/backups/drho/
- o /backups/g816prod/appl

Tape 1 Start:_____ End: _____

Verify ownership and permissions of backup files. They should be owned by the application ID/name.

- 5) Restore non /usr/users files needed for g816prod that aren’t restored using other methods. (Or could restore /oraappl/od-nbs/staging/dbarep from TSM)

☐ _____ initial

/usr/local/dr/siduser.dr -x -s g816prod

- 6) Restore any user files from systems other than zinc that were needed. Files should get restored from tape to /backups that will have a tar of user specific files needed.

☐ _____ initial

Run:

% sudo /usr/local/dr/siduser.dr -x -s iappprod

% sudo /usr/local/dr/siduser.dr -x -s igelprod

- 7) Reboot the system

☐ _____ initial

- 8) Let NBS know when the files have been restored

☐ _____ initial

Manual Instructions

Network Setup

Manually modify the following files:

ifconfig -a (to get network interface)

cd /var/root/etc

- o **sysconfigtab**

vi sysconfigtab (Update swap device, e.g. swapdevice=/dev/disk/dsk0b)

- **motd**
cp /etc/dr/system_files/motd.dr motd
- **fstab**
cp /etc/dr/system_files/fstab.dr fstab
vi fstab
 Verify the domain name and mount point for the boot disk.
 Verify tmp domain is defined.
 Verify no other mount point beside the boot disk.
- **hosts**
cp /etc/dr/system_files/hosts.dr hosts
vi hosts
 Verify hostname and IP
 (e.g. 165.112.213.240 dreos.cit.nih.gov dreos)
- **rc.config**
cp /etc/dr/system_files/rc.config.dr rc.config
vi rc.config

eos:

```
HOSTNAME="dreos.cit.nih.gov"
NUM_NETCONFIG="1"
NETDEV_0="tu2"
NETDEV_1=""
IFCONFIG_0="165.112.213.240 netmask 255.255.255.224"
IFCONFIG_1=""
GATED="no"
```

Original rc.config on eos

```
HOSTNAME="eos.nih.gov"
NUM_NETCONFIG="1"
NR_DEVICES="1"
NRDEV_0="nr0"
NRCONFIG_0="tu2,tu3"
IFCONFIG_0="128.231.56.102 netmask 255.255.254.0"
GATED="no"
```

lapis:

```
HOSTNAME="drlapis.cit.nih.gov"
NUM_NETCONFIG="1"
NETDEV_0="tu0"
NETDEV_1=""
IFCONFIG_0="128.231.164.3 netmask 255.255.255.248"
IFCONFIG_1=""
GATED="no"
```

garnet:

```
HOSTNAME="drgarnet.cit.nih.gov"
NUM_NETCONFIG="1"
NETDEV_0="tu0"
NETDEV_1=""
IFCONFIG_0="128.231.164.11 netmask 255.255.255.248"
IFCONFIG_1=""
GATED="no"
```

zinc:

```
HOSTNAME="drzinc.cit.nih.gov"
NUM_NETCONFIG="1"
NETDEV_0="tu2"
NETDEV_1=""
IFCONFIG_0="128.231.164.19 netmask 255.255.255.248"
NRDEV_0=""
NRDEV_1=""
NRCONFIG=""
NR_DEVICES=""
GATED="no"
```

```
# grep NR rc.config          (verify all netrain devices are removed – eos & copper)
# grep CONFIG rc.config      (verify network configurations)
```

○ **routes**

```
# cp /etc/dr/system_files/routes.dr routes
# vi routes
    Verify "default 165.112.213.225" for dreos
    Verify "default 128.231.164.9" for drgarnet
    Verify "default 128.231.164.1" for drlapis
    Verify "default 128.231.164.17" for drzinc
```

○ **inet.local**

```
# vi inet.local (drzinc only)
    Change network interface (e.g. "/usr/sbin/lan_config -i tu2 -a 0 -s 100 -x 1")
```

Start/Stop rc Scripts

Manually disable start/stop scripts as follows:

dreos

```
/var/root/sbin/rc0.d
• Disable: K01conndir, K01spongcl, K02oracle_ora, K03listctl
/var/root/sbin/rc0.d
• Disable: S40sendmail, S96class, S99conndir, S99spong2, S99spongcl, S99swatch
```

drlapis:

```
/var/root/sbin/rc0.d
• Disable: K01spongcl, K02oasctl
/var/root/sbin/rc3.d
• Disable: S92swatch, S98oasctl, S99spong2, S99spongcl
```

drgarnet:

```
/var/root/sbin/rc0.d
• Disable: K01conndir, K01spongcl, K02oracle_ora
/var/root/sbin/rc3.d
• Disable: S99conndir, S99spong2, S99spongcl, S99swatch
```

drzinc:

```
/var/root/sbin/rc0.d
```

- Disable: K01conndir, K01spongcl
/var/root/sbin/rc3.d
- Disable: S99spong2, S99spongcl, S99swatch

Boot Disk Configuration

Manually create file domains and filesets for the boot disk as follows:

```
# mkfdmn /dev/disk/dsk0d usr_dom
# mkfset usr_dom usr

# mkfdmn /dev/disk/dsk0e var_dom
# mkfset var_dom var

# mkfdmn /dev/disk/dsk0f tmp_dom
# mkfset tmp_dom tmp

# mkfdmn /dev/disk/dsk0g local_dom
# mkfset local_dom local

# mkdir /var/usr
# mount usr_dom#usr /var/usr

# mkdir /var/var /var/usr/local

# mount var_dom#var /var/var
# mount local_dom#local /var/usr/local
```

Dreos/drlapis/drzinc: (only)

```
# mkfdmn /dev/disk/dsk0h home_dom
# mkfset home_dom home
```

drlapis/drzinc: (only)

```
# mkdir /var/usr/users
# mount home_dom#home /var/usr/users
```

dreos: (only)

```
# mkdir /var/home
# mount home_dom#home /var/home
```

Fdmns Links setup

Manually setup the fdmns links as follows:

Remove old fdmns links

```
# cd /var/root/etc/fdmns
# rm -fr /var/root/etc/fdmns/*
```

Create new directory

```
# mkdir root_dom usr_dom var_dom tmp_dom local_dom
```

dreaos/drlapis/drzinc: (only)

```
# mkdir root_dom usr_dom var_dom tmp_dom local_dom home_dom
```

Create new directory

```
# cd root_dom
# ln -s /dev/disk/dsk0a
```

```
# cd ../var_dom
# ln -s /dev/disk/dsk0e
```

```
# cd ../tmp_dom
# ln -s /dev/disk/dsk0f
```

```
# cd ../local_dom
# ln -s /dev/disk/dsk0g
```

Dreos/drlapis/drzinc: (only)

```
# cd ..
# mkdir home_dom
# cd home_dom
# ln -s /dev/disk/dsk0h
```

Connect:Direct Setup

Manually modify the following files:

1) Install the DR license file (**license.key**)

```
% cd /usr/opt/conn_dir/ndm/cfg/[copper|eos|drgarnet].ndm
% cp /etc/dr/conn_dir/license.key.dr license.key
```

2) Modify netmap.cfg

```
% vi netmap.cfg
```

local.node:

```
:tcp.api=[drzinc|dreos|drgarnet].cit.nih.gov
[zinc|eos].ndm
:comm.info=[drzinc|dreos|drgarnet].cit.nih.gov
```

Copper: (**only**)

Add **nih.std.ndm** node (see netmap.cfg file for example of a node configuration)
:**comm.info**=165.112.213.229 (drtn3270.titan.nih.gov)

3) Modify ndmapi.cfg

```
# cd /usr/opt/conn_dir/ndm/cfg/cliapi
# vi ndmapi.cfg
```

api.parms:\

```
:tcp.hostname=[drcopper|dreos|drgarnet].cit.nih.gov:\
```

Gather system logs

Gather system logs and copy it over to eosrnde.

```
% cd /etc/dr
% sudo ./dr.collectlogs <path>
(e.g. dr.collectlogs /usr/users -or- where space available)
```

```
% cd <path>
(e.g. cd /usr/users)
% scp <hostname>_<mon><yr>.tar eosrnde:<path>
    Where <hostname> = drzinc, dreos, drgarnet, drlapis
(e.g. scp drcopper_Jul05.tar eosrnde:/usr/local/drlogs)
```

HP-UX

Last Modified: 4/16/07

Network Information

dr racer.cit.nih.gov 128.231.164.35
 default router 128.231.164.33
 netmask 255.255.255.248

racer.cit.nih.gov 128.231.92.142

Screen Commands

(start session as root so someone else can pick it up if needed)

% screen start screen session
 % screen -ls list the screen sessions
 CTRL-a d detach screen
 % screen -r attach screen
 % screen -r pid.tty.hostname attach specific screen session (if you have more than one open)

Set terminal type to vt100

CTRL - b
 GSP> he li
 GSP> ca (to set terminal type to vt100)
 GSP> co (return to console mode)

Restore from make_recovery tape

At the HP console Main Menu

```

----- Main Menu -----
Command          Description
-----
BObot [PRI|ALT|<path>]  Boot from specified path
PAth [PRI|ALT|<path>]   Display or Modify a path
SEArch [Display|IPL] [<path>] Search for boot device
CONfiguration menu    Displays or sets boot values
INformation menu      Displays hardware information
SERvice menu          Displays service commands
Help [<menu>|<command>] Displays help for menu or cmd
RESET                Restart the system
-----
Main Menu: Enter command or menu > sea (to search for tape device)

Path Number  Device Path (dec)  Device Type
-----
P0           10/0/6      Random Access Media
P1           10/0/5      Random Access Media
...
Main Menu: Enter Command or menu > boot p1
(p1 is the path to make_recovery tape drive)

Interact with IPL (y, n, or cancel)?> n

```

At the **Welcome the HP-UX installation/recovery process!** screen

```
[  _Install HP UX          ]
[  _Run a Recovery Shell  ]
[  _Advanced Options      ]
```

Select [Advanced Options]

At the **Advanced Options** screen

```
[  Show System Info          ]
[    Edit (vi) config file    ]
[  Edit (vi) environment vars ]
[ * ] Enable use of DHCP for network defaults
[ ^H ] Erase Character
[ 0 ] Debug Level
```

Disable use of DHCP by pressing the spacebar key to toggle the Enable and Disable

Select [OK] to get back to HP-UX installation/recovery screen.

At the **Welcome to the HP-UNIX installation/recovery process!** screen

```
[  _Install HP UX          ]
[  _Run a Recovery Shell  ]
[  _Advanced Options      ]
```

Select [I]nstall HP UX]

At the **User Interface and Media Options** screen

Source Location Options:

```
[ * ] Media only installation
[   ] Media with Network enabled (allow use of SD depots)
[   ] Ignite-UX server based installation
```

User Interface Options:

```
[   ] Guided Installation (recommended for basic installs)
[ * ] Advanced Installation (recommended for disk and file system management)
[   ] No user interface - use all the defaults and go
```

Set Media only installation for Source Location Options (as shown above)

Set Advanced Installation for User Interface Options (as shown above)

Select [OK] to continue

At **/opt/ignite/bin/rtool()** screen

```
/-----V-----V-----V-----V-----V-----\
| Basic || Software || System || File System || Advanced |
```

Select **Basic**

Change [Root Disk...] to the desired boot disk

Change [Root Swap (MB) ...] to the desired size

Select **System**

Change hostname to	drracer.cit.nih.gov
Change IP address to	128.231.164.35
Change Subnet Mask to	255.255.255.248

Set Root password

See the attached "Reference Section" to verify network information above.

Select **File System**

Change partition sizes as needed
(11/12/02 – keep the original partition sizes)

Select [Go!] to start the tape recovery.

...

Archive extraction from tape is beginning. Please wait.
(11/12/02 - at this point, it took about an hour and 25 minutes to complete)

After the tape recovery is completed, it returns to the "HP console Main Menu."

Main Menu: Enter command or menu > bo pri (to boot up the system)

(11/12/02 – it took about 40 minutes to boot)

When the machine comes up, login `drracer` and do the following:

- Review the log file (/etc/rc.log) for errors.
- Type **bdf** to verify file systems created on `drracer` are correct (see the attached bdf output of `racer`).
- Add the default router.

```
% sudo vi /etc/rc.config.d/netconf
Set ROUTE_GATEWAY=128.231.164.33
```

```
% netstat -nr
% ifconfig lan0
% sudo route add default 128.231.164.33 1
% sudo ifconfig lan0 up
```

- Ping out to verify network interface `lan0` is up.
- To check to see if lan card is set to 100 full duplex run : `lanadmin -x lan0`
- To set the lan card to 100 full duplex run (this automatically means auto negotiation is off:
`lanadmin -X FD100 lan0`
- If the network connection is not set to 100 Mbs full duplex, then set the Network Card configuration to 100 Full duplex, this is how to do it in sam.

```
% sudo sam
Select "Networking and Communications"
Select "Network Interface Cards"
Select "Actions" and "Modify"
```

Set Autoneg: **OFF**
 Set Speed (million bps): **100**
 Set Duplex Mode: **FULL**

Select OK to save
 Exit sam

- Verify drracer entry in /etc/hosts file.

```
128.231.164.35      drracer.cit.nih.gov      drracer
```

- Remove -a flag from /etc/inetd.conf

```
% sudo vi /etc/inetd.conf
Search ftp entry
      ftp  stream  tcp  nowait  root  /usr/local/etc/tcp  ftpd -oil -a
Remove "-a" at the end of ftp
```

Restart inetd
 % sudo -HUP inet

Prepare for Application Restores

- 1) Create physical volumes if necessary

☐ _____ initial

```
# ioscan -funC disk > ioscan.out
edit ioscan.out, leaving a list of only UNCLAIMED raw devices
(/dev/rdisk/c#t#d#)
run pvcreate -f for all items in the list
# for x in `cat ioscan.out.mod`
do
    pvcreate -f $x
done
```

- 2) Create a new volume group for application restore (in this step you can choose to create several volume groups. the number of volume groups will be determined by the size of each disk.)

☐ _____ initial

The format of the command that will be used to create the new volume group or vg is:

```
/usr/sbin/vgcreate [-f] [-A autobackup] [-x extensibility] [-e max_pe]
                  [-l max_lv] [-p max_pv] [-s pe_size] [-g pvg_name] vg_name
                  pv_path ...
```

The pv_path are the disk paths that will be used in the vg. Use the disks from ioscan.out.mod to find out what size the disks you will use to create a new vg are. The disk size will help approximate what pe size and max pv you will need. Use the name of each disk to see what size the disks are by running the below for loop.

```
# for x in `cat ioscan.out.mod`
do
```

```
diskinfo $x >> /tmp/dsize
done
```

Edit the /tmp/dsize file to look at the disk sizes, most likely the disks will be all one size. As an example disks of 35GB will be used though the document.

The size of the disk is a consideration in creating a vg as there are hard limits set by the logical volume manager per volume group. The major factor is usually the hard limit set on maximum physical extents a volume group is allowed to have. A physical extent is basically a chunk of disk in megabytes that the volume manager of the OS logically divides the disk in at vg creation.

For instance if the physical extent or PE is left at 4MB which is the default on a 35GB disk that means each disk can have a maximum of 8750 PEs. The hard limit of PEs per entire volume group that is allowed is 65535, so that means that if the PE is left at 4MB there can be only up to seven 35GB disks allocated to a volume group if all the disks are 35GB. Otherwise another disk would push the limit of the PE beyond 65535 and this is not allowed by the OS. ($65535 / 8750 = 7.49$)

So you can pick a small PE as long as you have a small set of disks per volume group or another option is to have a larger PE size which will allow more disks in the vg.

For example picking a larger PE of size 32MB per 35GB disk would yield a PE max of number of 1093 PEs per disk. This would mean that it would take about 59 35GB disks to reach the 65535 limit of max PEs per volume group. ($65535 / 1093 = 59.95$).

The next step is to place the command in a script to run later. Edit a file called vgcr1.scr and place each of the disk device paths from ioscan.out.mod but modify the dev path with "rdsk" where "disk" is listed. Then add the vgcreate and it's options just before the list of disk paths in the script. The script should look something like this the sizes will change depending on your disk sizes and your choice of PE per disk:

```
vgcreate -e <max pe or 65535> -max_lv <number of logical volumes to be assigned to this vg> -p
<number of maximum disks per vg> -s <PE size> <vg name> <disk names from ioscan.out.mod>
```

Assuming that each disk is 35GB:

```
>view vgcreate.scr
```

```
vgcreate -e 65535 -max_lv 100 -p 50 -s 32 vg04 /dev/rdsk/c5t0d0 /dev/dsk/c5t1d0 /dev/rdsk/c5t2d0
/dev/dsk/c5t3d0 /dev/rdsk/c5t4d0 /dev/dsk/c5t5d0 /dev/rdsk/c5t6d0 /dev/dsk/c5t7d0 /dev/rdsk/c5t8d0
/dev/dsk/c5t9d0 /dev/rdsk/c5t10d0 /dev/dsk/c5t11d0
```

Save the vgcreate.scr and change it's permissions so it's executable.

Remove any reference to existing logical volume

```
# rm -rf /dev/vg04 - this is to remove reference to old vg04
```

Create new volume group

```
# mkdir /dev/vg04
```

```
# cd /dev/vg04
```

```
# grep group /dev/*/group - Look at the 0x000000 pattern numbers listed and choose a unique
number not listed for the next step
```

```
# mknod group c 64 0x040000 - make sure number is unique
```

```
# ./vgcreate.scr
```

3) Create logical volumes for /u01 to /u17, /opt/psoft8, /opt/app/oracle and /backups:

☐ _____ initial

(Modify /etc/dr/dr.makelv to change volume group to vg04)
Execute the script **/etc/dr/dr.makelv**

% sudo /etc/dr/dr.makelv vg04

OR manually create the logical volumes:

Create logical volume /u01 to /u17

```
% sudo /usr/sbin/lvcreate -L 10240 vg04
% sudo /usr/sbin/newfs -F vxfs -o largefiles /dev/vg04/rlvol1
% sudo /usr/bin/mount /dev/vg04/lvol1 /u01
```

Repeat the commands above (lvcreate, newfs and mount) to create logical volumes from 1 through 17 (lvol1, lvol2, ... lvol17). Remember to use -o largefiles option.

Create logical volume for /opt/psoft8 and /opt/app/oracle and /backups/

```
% sudo mkdir -p /opt/psoft8 /opt/app/oracle /backups
% sudo /usr/sbin/lvcreate -L 15000 vg04
% sudo /usr/sbin/newfs -F vxfs -o largefiles /dev/vg04/rlvol18
% sudo /usr/sbin/mount /dev/vg04/lvol16 /opt/psoft8
```

```
% sudo /usr/sbin/lvcreate -L 4000 vg04
% sudo /usr/sbin/newfs -F vxfs -o largefiles /dev/vg01/rlvol19
% sudo /usr/sbin/mount /dev/vg04/lvol17 /opt/app/oracle
```

```
% sudo /usr/sbin/lvcreate -L 1000 vg04
% sudo /usr/sbin/newfs -F vxfs -o largefiles /dev/vg01/rlvol20
% sudo /usr/sbin/mount /dev/vg04/lvol18 /backups
```

4) Create directories under the mount points.

☐ _____ initial

Execute the script **/etc/dr/dr.makedir**

OR manually create the directories:

```
/u01/oradata/EHRPPRD
/u02/oradata/EHRPPRD
/u03/oradata/EHRPPRD
/u04/oradata/EHRPPRD
/u05/oradata/EHRPPRD
/u06/oradata/EHRPPRD
/u07/oradata/EHRPPRD
/u08/oradata/EHRPPRD
/u09/oradata/EHRPPRD
/u10/oradata/EHRPPRD
/u11/oradata/EHRPPRD
/u12/oradata/EHRPPRD
/u13/oradata/EHRPPRD
/u14/oradata/EHRPPRD
/u14/oradata/EHRPPRD
/u15/oradata/EHRPPRD
/u16/oradata/EHRPPRD
/u17/oradata/EHRPPRD
/opt/psoft8
```

/opt/app/oracle
/backups/oradata/drtest

- 5) Modify the **/etc/fstab** as needed.

☐ _____ initial

- 6) Unlock and reset password for account psoft8

☐ _____ initial

% sudo /usr/sbin/modprpw -k psoft8

- 7) Add drracer to **/etc/hosts.allow**: allow drracer to ftp to itself (emulating cobra to viper)
Uncomment from /etc/hosts.allow, lines after “ENTRIES FOR DR TESTING”

☐ _____ initial

- 8) Comment out tsm restart (dsm.runchk) from **cron**

☐ _____ initial

- 9) Modify **dsm.sys**.

☐ _____ initial

% cd /opt/tivoli/tsm/client/ba/bin
% sudo vi dsm.sys

Change **NodeName** from racer to drracer in the stanza(s) for the TSM server that will be used. If the production TSM server at NIH is used, the “aixtsm” stanza needs to be changed. If TSM has been restored offsite, then the “dr” stanza needs to be changed.

- 10) Modify **/etc/sudoers** – uncomment lines at end for psoft8

☐ _____ initial

PSC ALL=/pt/psoft8/pt819/start_WebLogic.sh
psoft8 ALL=/pt/psoft8/pt819/start_WebLogic.sh

OR add psoft8 to PSC group in sudoers file and add or uncomment the line:

PSC ALL=/pt/psoft8/pt819/start_WebLogic.sh

- 11) Notify Adrienne that the system is up and ready for application restores.

☐ _____ initial

Restore Customer Applications

- 1) Start a script session to document any commands run.

☐ _____ initial

- 2) Restore /opt/app/oracle and /backups/drtest from tape. Ask for tape “racer sysbackup.app”.

☐ _____ initial

Run the script “/usr/local/dr/apprestore” to restore the directories /opt/app/oracle and /backups/oradata/drtest. Make sure you use the non-rewinding tape designation. (i.e. /dev/rmt/0mn)

```
# /usr/local/dr/apprestore -d DEV
```

OR manually restore as follows:

```
# mt -f DEV rewind
# cd /opt/app/oracle
# vxrestore -f DEV-vx
Vxfs vxrestore warning: ./lost+found: File exists
Vxfs vxrestore: you have not read any tapes yet.
Unless you know which volume your file(s) are on you should start with the last volume and work
towards the first
Specify next volume #: 1

# cd /backups
# vxrestore -f DEV -vx ./oradata/drtest
```

Restore times:

Start:_____ End: _____

- 3) Restore /opt/psoft8 from cobra. Ask for tape “cobra cobra.app”. This is a DLT tape so it will be mounted in a different drive from the racer tapes.

☐ _____ initial

```
# mt -f DEV rewind
# cd /opt/psoft8
# vxrestore -f DEV
Specify next volume # : 1
Set owner mode for . ? [yn] y
```

Restore times:

Start:_____ End: _____

- 4) Update the DR web page and notify EHRP when restore is complete

☐ _____ initial

Command Syntax References

A) vgcreate(1M)

NAME

vgcreate - create LVM volume group

SYNOPSIS

```
/usr/sbin/vgcreate [-f] [-A autobackup] [-x extensibility] [-e max_pe]
```

`[-l max_lv] [-p max_pv] [-s pe_size] [-g pvg_name] vg_name pv_path ...`

DESCRIPTION

The `vgcreate` command creates a new volume group. `vg_name` is a symbolic name for the volume group and must be used in all references to it. `vg_name` is the path to a directory entry under `/dev` which must contain a character special file named `group`. Except for the group entry, the directory `vg_name` should be empty. The `vg_name` directory and the group file have to be created by the user (see `lvm(7)`).

`vgcreate` leaves the volume group in an active state.

Before assigning a physical volume to a volume group, the physical volume has to be created using the `pvcreate` command (see `pvcreate(1M)`).

If `vgcreate` fails to install the first specified physical volume into the volume group, the volume group is not created. If, for any reason, one of the remaining specified physical volumes cannot be installed into the volume group, an error message is printed, but the installation continues until the end of the list of physical volumes.

Options and Arguments

`vgcreate` recognizes the following options and arguments:

<code>pv_path</code>	The block device path name of a physical volume that will be assigned to the new volume group. You can specify physical volume links (pv-links) for a physical volume providing different paths that reference the same physical volume in the <code>pv_path</code> list. The order in which the paths are listed is important. The first path becomes the primary link to the physical volume, the second becomes an alternate link to the physical volume. The primary link is the default path used to access the physical volume. If the primary link becomes unavailable, LVM automatically switches to the alternate link to access the physical volume. Currently LVM supports a maximum of 8 paths to a physical volume (7 alternate and one primary).
<code>vg_name</code>	The path name of a subdirectory of the <code>/dev</code> directory. <code>vg_name</code> must be empty except for a character special file named <code>group</code> . Typically, this directory name is in the form <code>/dev/vgNN</code> , where <code>NN</code> numbers sequentially from 00.
<code>-A autobackup</code>	Set automatic backup for this invocation of this command. <code>autobackup</code> can have one of the following values: <ul style="list-style-type: none"> <code>y</code> Automatically back up configuration changes made to the volume group. This is the default After this command executes, the <code>vgcfgbackup</code> command (see <code>vgcfgbackup (1M)</code>) is executed for the volume group. <code>n</code> Do not back up configuration changes this time.
<code>-e max_pe</code>	Set the maximum number of physical extents that can be allocated from any of the physical volumes in the volume group. The default value for <code>max_pe</code> is 1016. However, if the size of any physical volume exceeds 1016 times the <code>pe_size</code> , the default value for <code>max_pe</code> is adjusted to match the physical volume size. The maximum number of physical extents can be a value in the range 1 to 65535.
<code>-f</code>	This option will force a volume group to be created with a physical volume

which has alternate block(s) already allocated, (i.e. this physical volume was not initialized using pvcreate -f.) This option should be used with extreme caution. If the volume group to be created has a different physical extent size, the alternate block(s) might be inside the user data area. Potential data corruption could occur.

- g pvg_name Create a new physical volume group with the name pvg_name. All physical volumes specified in the pv_path parameter become a member of the newly created physical volume group.

The physical volume group information is stored in an ASCII file, /etc/lvmpvg. The file can be edited to create a physical volume group instead of using the vgcreate command. However, ensure that the physical volumes to be used have already been installed in the volume group prior to creating the physical volume group.

The physical volume group name must be unique within a volume group although identical physical volume group names can appear in different volume groups (see lvmpvg(4) for format details).
- l max_lv Set the maximum number of logical volumes that the volume group is allowed to contain. The default value for max_lv is 255. The maximum number of logical volumes can be a value in the range 1 to 255.
- p max_pv Set the maximum number of physical volumes that the volume group is allowed to contain. The default value for max_pv is 16. The maximum number of physical volumes can be a value in the range 1 to 255.
- s pe_size Sets the number of megabytes in each physical extent, where pe_size is expressed in units of megabytes (MB) in the range 1 to 256. pe_size must be equal to a power of 2 (1, 2, 4, 8, etc.). The default value for pe_size is 4 (four megabytes).
- x extensibility Set the allocation permission for adding physical extents on the physical volumes specified by the pv_path parameter. extensibility can have one of the following values:
 - y Allow allocation of additional physical extents on the physical volume. This is the default.
 - n Prohibit allocation of additional physical extents on the physical volume. Logical volumes residing on the physical volume can still be accessed after the volume group has been activated by the vgchange -a y command.

EXTERNAL INFLUENCES

Environment Variables

LANG determines the language in which messages are displayed.

If LANG is not specified or is null, it defaults to "C" (see lang(5)).

If any internationalization variable contains an invalid setting, all internationalization variables default to "C" (see environ(5)).

EXAMPLES

Create a volume group named /dev/vg00 containing two physical volumes with extent size set to 2 MB, from scratch.

First, create the directory /dev/vg00 with the character special file called group.

```
mkdir /dev/vg00
mknod /dev/vg00/group c 64 0x030000
```

The minor number for the group file should be unique among all the volume groups on the system. It has the format 0xNN0000, where NN runs from 00 to 09. The maximum value of NN is controlled by the kernel tunable parameter maxvgs.

Initialize the disks using pvcreate(1M).

```
pvcreate /dev/rdisk/c1t0d0
pvcreate /dev/rdisk/c1t2d0
```

Create the volume group.

```
vgcreate -s 2 /dev/vg00 /dev/dsk/c1t0d0 /dev/dsk/c1t2d0
```

Create a volume group named /dev/vg01 that can contain a maximum of three logical volumes, with extent size set to 8 MB:

```
vgcreate -l 3 -s 8 /dev/vg01 /dev/dsk/c3t4d0
```

Create a volume group named /dev/vg00 and a physical volume group named PVG0 with two physical volumes:

```
vgcreate -g PVG0 /dev/vg00 /dev/dsk/c1t0d0 /dev/dsk/c2t0d0
```

Using the PVLinks feature to create a volume group named /dev/vg00 with a physical volume which can be referenced by two different paths. /dev/dsk/c3t0d0 and /dev/dsk/c4t0d0 refer to the same physical volume, accessed via different controller hardware paths. In this example, /dev/dsk/c3t0d0 becomes the primary link to the physical volume. /dev/dsk/c4t0d0 becomes an alternate link to the physical volume.

```
vgcreate /dev/vg00 /dev/dsk/c3t0d0 /dev/dsk/c4t0d0
```

WARNINGS

It is not possible to create a volume group that contains both HP-IB devices and devices using another type of interface.

B) Extending a jfs filesystem on-line

```
Fsadm -F vxfs -b <entire new size of filesystem in MB = current size + increase>M <mountpoint>
```

Example:

```
Fsadm -F vxfs -b 4000M /u01
```

Gather system logs

Gather system logs and copy it over to eosrnde.

```
% cd /etc/drsun
% sudo ./dr.collectlogs <path>
    (e.g. dr.collectlogs /home –or- where space available)
% cd <path>
    (e.g. cd /home)
% scp drracer_<mon><yr>.tar eosrnde:<path>
    (e.g. scp drracer_Jul05.tar eosrnde:/usr/local/drlogs)
```

Solaris

Last Modified: 7/10/07

Network Information

drdanica.cit.nih.gov	128.231.164.20
drandretti.cit.nih.gov	128.231.164.21
default router	128.231.164.17
netmask	255.255.255.248
drandromeda.cit.nih.gov	128.231.164.27
default router	128.231.164.25
netmask	255.255.255.248
drcorvus.cit.nih.gov	165.112.213.238
drpuppis.cit.nih.gov	165.112.213.239
drafpasp.cit.nih.gov	165.112.213.242
default router	165.112.213.225
netmask	255.255.255.224
drweb1.cit.nih.gov	137.187.22.118
drcrisp.cit.nih.gov	137.187.22.126 (virtual host of drweb1)
default router	137.187.22.65
netmask	255.255.255.192

Screen Commands

% screen	start screen session
% screen -ls	list the screen sessions
CTRL-a d	detach screen
% screen -r	attach screen
% screen -r pid.tty.hostname	attach specific screen session (if you have more than one open)

Define console

Local> prompt
 Type show serv
 Type connect wdpcm1

Username: ccs
 Password: ccs

Type ccon <conn_name>

The point-of-contact of SUN servers will tell you the connection name and network interface to use for each system. Write the information below on the white board for reference.

	Connection	Network Interface
drdanica (V880)	_____	_____
drandretti (280R)	_____	_____
drandromeda (E420R)	_____	_____

drcorvus (280R) _____ _____
drafpdp (UE 5000) _____ _____
(drweb1)

**** drafpdp is part of drweb1; drweb1 is being restored at NIH ****
**** drandretti is drpuppis; the system was borrowed from ERA ******Build system**

Build the System

The **drsun** image directory is saved in /usr/local/drsun on eosrnde.

Skip this section if the system is being built at NIH.

Check and initial after each step is completed.

1) Logon as root.

☐ _____ initial

2) Untar tar file 'drsun.tar'.

☐ _____ initial

Ask to have the CD "**DRSUN V2.1**" put in the CDROM drive.

Find a directory with the most space to untar the tar files for sscripts, patches, and java..

Untar *drsun.tar*

```
# cd <path>
# tar xf /cdrom/cdrom0/drsun.tar
# cd <path>/drsun
# tar xf SunOS.tar
```

Untar *patches.tar*

```
# cd <path>
# tar xf /cdrom/cdrom0/patches.tar
```

Untar *Java.tar*

```
# cd <path>
# tar xf /cdrom/cdrom0/Java.tar
```

drandromeda: (only)

Because drandromeda does not have DVD drive, you need to put in a total of 3 CDs to retrieve all the tar files.

Find a directory with the most space to untar the tar files for sscripts, patches, and java.

Ask to have the CD "**drsun 7/07**" put in the CDROM drive.

Untar *drsun.tar*

```
# cd <path>
# tar xf /cdrom/cdrom0/drsun.tar
# cd <path>/drsun
```

```
# tar xf SunOS.tar
```

Ask to have the CD “**patches 7/07**” put in the CDROM drive.

```
Untar patches.tar  
# cd <path>  
# tar xf /cdrom/cdrom0/patches.tar
```

Ask to have the CD “**Java 7/07**” put in the CDROM drive.

```
Untar Java.tar  
# cd <path>  
# tar xf /cdrom/cdrom0/Java.tar
```

3) Add oracle settings to /etc/system file.

☐ _____ initial

drdanica: (only)

```
# cd <path>/drsun/drdanica  
# .dr.os_system
```

4) Install patches.

☐ _____ initial

```
# cd <path>/patches  
# cd 5.9  
# unzip 9_Recommended.zip  
# cd 9_Recommended  
# .install_cluster  
# tar xf Misc_patches.tar  
# cd Misc_patches  
# .installpatches.ksh
```

5) Reboot the system.

☐ _____ initial

```
# init 6
```

6) Verify the network is up.

☐ _____ initial

```
% ping eosrnde
```

If the network is not up, then do the following:

a) Copy the network files to the system

```
# cd <path>/drsun  
# .dr.os_netfiles <hostname>  
Where <hostname> = drandromeda, drandretti, drdanica, drcorvus, drafp
```

(Notes: you must run the script above from the *drsun* directory)

OR manually modify the following files in */etc* directory: *resolv.conf*, *nsswitch.conf*, *hosts*, *defaultrouter*, and *netmasks*.

b) Bring up the network interface

```
# ifconfig -a      (to get the network interface)
# cd <hostname>
    Where <hostname> = drandromeda, drandretti, drdanica, drcorvus, drafpasp
# ./dr.os_netup
```

(OR) manually bring up the network interface:

```
# ifconfig -a
# route add default <default router> 1
# ifconfig <network interface> down
# ifconfig <network interface> inet <IP> netmask <netmask ip>
# ifconfig <network interface> up
```

Reboot the system if the network is not up.

7) Check system date.

☐ _____ initial

date

If the time zone is other than **EST** or **EDT**, then it need to be changed.

vi /etc/TIMEZONE

Change "TZ=US/Central" to "TZ=US/Eastern"

The system needs a reboot for the change to take effect, but do not reboot the system at this time.
The system will get rebooted after the patches are installed.

8) Install software packages.

☐ _____ initial

Shutdown sshd daemon that comes with Solaris 9

pkill sshd

Run script below to install software packages:

```
# cd <path>/drsun
```

```
# ./dr.os_pkgadd
```

OR manually install the software packages in **Sol5.9_pkgs**:

☐ Verify */usr/local/sbin/sshd* is running (*ps -ef | grep sshd*)

9) Get location of home directory.

☐ _____ initial

Find the location of home directory. It can be a separate partition or part of another partition depending the system setup.

```
% df -k
% ls /home /export/home
```

If **/home** directory is used as the home directory, do the following:

```
% sudo vi /etc/auto_master
Comment out the /home entry in this file
% sudo /etc/init.d/autofs stop
% sudo /etc/init.d/autofs start
% sudo chmod 755 /home
```

10) Run mini-admin setup.

☐ _____ initial

```
# cd <path>/drsun
# ls SunOS (to verify SunOS directory is untar)
# ./dr.os_admsetup <hostname>
Where <hostname> = drandromeda, drandretti, drdanica, drcorvus, drafpsp
```

The script above copies customized files such as hosts.allow, sudoers, ntp.conf, pam.conf, etc.

11) Create admin accounts.

☐ _____ initial

```
# cd <path>/drsun
# df -k
Get the home directory path
```

Create admin accounts:

```
# ./dr.os_admaccts <home_directory>
(e.g. dr.os_admaccts /export/home)
```

Setup admin accounts (creates .forward and copy .profiles/.cshrc files)

```
# cd SunOS
# ./setup_admin_accts
```

12) Create dba accounts.

☐ _____ initial

drafpsp, drweb1 (@NIH): (only)

```
# cd <path>/drsun/<hostname>
Where /<hostname> = drafpsp, drweb1
# df -k
Get the home directory path
# ./dr.app_accts <home_directory>
(e.g. dr.app_accts /export/home)
```

13) Install Java.

drdanica, drandretti: (only)

☐ _____ initial

Install Java 1.3.1_19 and make it as the default

```
# cd /usr
# tar xf <path>/Java/java1.3.1_19.tar
# mv java java.orig
# ln -s java1.3.1_19 java
```

drdanica: (only)

Install Java 1.4.2_08

```
# cd /usr
# tar xf <path>/Java/jdk.tar
```

drandretti: (only)

Install Java 1.4.2_10

```
# cd /usr
# tar xf <path>/Java/java1.4.2_10.tar
```

drandromeda, drafpsp, drweb1 (@NIH):

☐ _____ initial

Install Java 1.5.0_11 and make it as the default

```
# cd /usr
# tar xf <path>/Java/java1.5.0_11.tar
# mv java java.orig
# ln -s java1.5.0_11 java
```

14) Install X11R6

☐ _____ initial

drdanica, drandretti, drcorvus, drafpsp, drweb1 (@ NIH):

```
# cd <path>/drsun
# ./dr.os_installX11
```

Verify xvfb is running

```
# ps -ef | grep -i xvfb
```

You should see "/usr/X11R6/bin/Xvfb :1" process running

Prepare for Application Restores

Use Veritas file system for **drbiffle** and **drpenske**.

Use Sun Volume Management for **drandromeda**, **drcorvus**, and **drafpsp**

1) Create accounts

☐ _____ initial

```
# cd <path>/drsun/<hostname>
Where /<hostname> = drandromeda, drandretti, drdanica, drcorvus, drafpasp
# df -k
Get the home directory path
# ./dr.app_accts <home_directory>
(e.g. dr.app_accts /export/home)
```

2) Install Veritas

☐ _____ initial

drandretti, drdanica: (only)

This step only applies to **drandretti** and **drdanica**.

- Install Veritas software by following the document “**Veritas Storage Foundation for Oracle installation**”

Request the following CDs mounted in the following order:

SF V4.1 Disk 01
SF V4.1 Disk 02
SF V4.1 Disk 03

- Install Veritas temporary license

Temporary license for 7/07 test:

RJPG-NPCZ-H7MH-VL4I-HSFT-ONCC-O6 for **drandretti** and **drdanica**

3) Create Veritas disk group.

☐ _____ initial

This step is for **drandretti** and **drdanica** only.

Before you begin, verify the following directories are in your path:

/opt/VRTS/bin:/opt/VRTSob/bin:/usr/lib/vxvm/bin

Veritas commands

```
# vxdisk list -o alldgs list (List all disks including deported disk groups)
# vxprint -g <grpname> (List logical volumes and internal group names)
# vxprint -g <grpname> | grep ^v (List logical volumes)
# vxassist -g <grpname> maxsize (List current available size of a disk group)
# vxassist -g <grpname> help space \
| grep "Disk:" (List all free space of a disk group)
# vxresize -g <grpname> <volname> \
[50m | +50m | -50m ] (Set 50mb | add by 50mb | shrink by 50mb)
```

drandretti: (7/07)

Application main directory : **/oraappl/od-nbs/staging/dbaproj**

Disk size requirement : 100 MB

Application main directory : **/oraappl/od-nbs/a159prod**
 Disk size requirement : 40 GB

Application main directory : **/oraappl/od-nbs/s380prod**
 Disk size requirement : 15 GB

Application main directory : **/oraappl/od-nbs/m551prod**
 Disk size requirement : 5 GB

Application main directory : **/oraappl/od-nbs/backups**
 Disk size requirement : 50 GB

The space requirement for **/var/opt/oracle** directory is small enough that it going to be part of the boot disk.

Format the disk

% sudo format
 (Label all the disks you need for ~150GB space requirement)

Initialize the disk

% sudo /opt/VRTS/bin/**vxdiskadm**

Select an operation to perform: **1**
 (type 1 to select "Add or initialize one or more disks")

Type in the disk pattern type **list** to see the list of disks;
 Add the disk the disk group "**drandretti_dg**"

(OR) create the disk group using **vx dg** command

% sudo **vx dg init** drandretti_dg <disk_device1>
 % sudo **vx dg -g** drandretti_dg **add disk** <disk_device2> <disk_device3> ...

NOTES: Make sure you name the disk group "**drandretti_dg**" or the script that create volumes will not work.

Verify the disks are intiaized and disk group is created

% **vx disk list -o alldgs list**

drdanica: (7/07)

Application main directory : **/oraappl/od-nbs/staging/dbaproj**
 Disk size requirement : 100 MB

Application main directory : **/oraappl/od-nbs/a159prod**
 Disk size requirement : 500 GB

Application main directory : **/oraappl/od-nbs/s380prod**
 Disk size requirement : 40 GB

Application main directory : **/oraappl/od-nbs/c500prod**
 Disk size requirement : 30 GB

Application main directory : **/oraappl/od-nbs/backups**
 Disk size requirement : 300 GB

The space requirement for **/var/opt/oracle** directory is small enough that it going to be part of the boot disk.

Format the disk

% sudo format
(Label all the disks you need for ~900GB space requirement)

Initialize the disk

% sudo /opt/VRTS/bin/**vxdiskadm**

Select an operation to perform: **1**
(type 1 to select “Add or initialize one or more disks”)

Type in the disk pattern type **list** to see the list of disks;
Add the disk the disk group “**drdanica_dg**”

(OR) create the disk group using **vx dg** command

% sudo **vx dg init** drdanica_dg <disk_device1>

% sudo **vx dg -g** drdanica_dg **add disk** <disk_device2> <disk_device3> ...

NOTES: Make sure you name the disk group “**drdanica_dg**” or the script that create volumes will not work.

Verify the disks are intiaized and disk group is created

% **vx disk list -o alldgs list**

4) Create *Veritas* volumes.

☐ _____ initial

This step is for **drandretti** and **drdanica** only.

drandretti: (7/07)

cd <path>/drsun

cd *drandretti*

./dr.app_vols

The script creates the following volumes:

a159prod, s380prod, m551prod, staging, backups

drdanica: (7/07)

cd <path>/drsun

d *drdanica*

./dr.app_vols

The script creates the following volumes:

a159prod, s380prod, c500prod, staging, backups

5) Prepare the disk for application directories.

☐ _____ initial

This step is for **drandromeda**, **drcorvus** and **drafpasp** only.

Use the instructions below to create the application directories:

- Run **format** to determine the sizes of the available disks.
- Pick a disk for each directory that is large enough for the data restore.
- Pick a partition number 3,4,5,6 or 7 for the application directory
- Write down the file system for each application directory.
- Remember to type **label** at the main format menu to save the changes.
- Run **newfs** and **fsck** on the new partitioned disks

Example:

```
# newfs /dev/dsk/c0t8d0s4
```

```
# fsck /dev/dsk/c0t8d0s4
```

Notes: If the disk requirement size is larger than the size of the disk, then you need to concatenate the disks. See "Concatenate disks using SVM" section below for instructions.

drandromeda: (7/07)

Application main directory : **/oraappl/od-nbs/w133prod**

Disk size requirement : 500 MB

drcorvus: (7/07)

Application main directory : **/opt/oracle**

Disk size requirement : 25 GB

File system : _____

Application main directory : **/oracle/apps**

Disk size requirement : 3 GB

File system : _____

drafpasp: (7/07) – afpasp only

Application main directory : **/oramount**

size requirement : 12 GB

Disk File system : _____

Application main directory : **/backups**

Disk size requirement : 5 GB

File system : _____

drweb1 (restore @ NIH) – restore afpasp and crispas

Application main directory : **/oramount**

size requirement : 20 GB

Disk File system : _____

Application main directory : **/backups**

Disk size requirement : 5 GB

File system : _____

Application main directory : **/apps**

Disk size requirement : 5 GB

File system : _____

Concatenate disks using SVM

The procedures below are for disk concatenation.

***** Skip this section if the disks are large enough for application data *****

Example: If an individual disk size is 8GB and the total required disk size is 30GB, then 4 disks need to be concatenated.

```
Create the meta database
# metadb -i
# metadb -a -c3 -f c0t1d0s7
(substitute the controller, target# and slice# for meta database accordingly)
```

```
Concatenate the disk
# metainit d20 4 1 c0t2d0s2 1 c0t3d0s2 1 c0t4d0s2 1 c0t5d0s2
# vi /etc/vfstab
Add "/dev/md/dsk/d20 /dev/md/rdisk/d20 /apps ufs 2 yes -"
% mkdir /apps
% sudo mount /apps
% sudo growfs -M /apps /dev/md/rdisk/d20
```

6) Create application directories and mount the file systems.

NOTES: Make sure to 'cd' to the host director before running *dr.app_dirs* script.

drandretti:

☐ _____ initial

```
# cd <path>/drsun/drandretti
# ./dr.app_dirs
```

The script do the following:

- A) creates and mount the application directories
- B) updates /etc/vfstab file
- C) untar /var/opt/oracle directory
- D) untar /oraappl/od-nbs/staging/dbaproj

drdanica:

☐ _____ initial

```
# cd <path>/drsun/drdanica
# ./dr.app_dirs
```

The script do the following:

- A) creates and mount the application directories
- B) updates /etc/vfstab file
- C) untar /var/opt/oracle directory
- D) untar /oraappl/od-nbs/staging/dbaproj

drandromeda:

☐ _____ initial

- Create application root directory.

```
# mkdir -p /oraappl/od-nbs
# chmod 755 /oraappl/od-nbs
```

```
# vi /etc/vfstab
```

Add the disk device for the following directory:

```
/dev/dsk/cctxdxsx /dev/rdsk/cctxdxsx /oraappl/od-nbs ufs 2 yes logging
```

☐ Verify permission of /oraappl directory is 755 before mounting

```
# mount /oraappl/od-nbs
```

- Create application directory.

```
# cd <path>/drsun/drandromeda
```

```
# ./dr.app_dirs
```

The script:

```
creates /oraappl/od-nbs/w133prod directory
changes owner on /oraappl/od-nbs/w133prod directory
```

drcorvus:

☐ _____ initial

- Create application root directories.

```
# mkdir -p /opt/oracle
# mkdir -p /oracle/apps
# chmod 755 /opt/oracle /oracle/apps
```

```
# vi /etc/vfstab
```

Add the disk device for the following directory:

```
/dev/dsk/cctxdxsx /dev/rdsk/cctxdxsx /opt/oracle ufs 2 yes logging
/dev/dsk/cctxdxsx /dev/rdsk/cctxdxsx /oracle/apps ufs 2 yes logging
```

☐ Verify permission of /opt/oracle and /oracle/apps directories are 755 before mounting

```
# mount /opt/oracle
# mount /oracle/apps
```

- Create application directories

```
# cd <path>/drsun/drcorvus
```

```
# ./dr.app_dirs
```

The script:

```
creates /apps/oracle/apps/swlib directory
changes owner on /opt/oracle directory
```

drafpdp: - restore afpdp only

☐ _____ initial

- Create application root directories

```
# mkdir /oramount
# mkdir /backups
# chmod 755 /oramount /backups
```

```
# vi /etc/vfstab
```

Add the disk device for the following directories:

```
/dev/dsk/cctxdxsx /dev/rdisk/cctxdxsx /oramount ufs 2 yes logging
/dev/dsk/cctxdxsx /dev/rdisk/cctxdxsx /backups ufs 2 yes logging
```

- ☐ Verify permission of /oramount and /backups directories are 755 before mounting

```
# mount /oramount
# mount /backups
```

- Create application directories

```
# cd <path>/drsun/drafpdp
```

```
# ./dr.app_dirs
```

The script:

```
creates /oramount/oramaint/[orasoft_polaris,others_polaris] directory
creates /oramount/orabin/dfo-afps/afpspoas directory
creates /oramount/oracle/dfo-afps/afpspoas directory
creates /backups/OAS/afpsppoas directory
untar /usr/local/oracle, /var/opt/oracle, /oramount/oramaint/scripts
link /oramount/orabin to /orabin
link /oramount/oracle to /oracle
```

drweb1: (restore @ NIH) – restore afpdp & crispas

☐ _____ initial

Three common directories on polaris and pisces: /usr/local/oracle, /var/opt/oracle, /oramount/oramaint/scripts – these directories should be restored from polaris.

- Create application root directories

```
# mkdir /oramount
# mkdir /backups
# mkdir /apps
# chmod 755 /oramount /backups /apps
```

```
# vi /etc/vfstab
```

Add the disk device for the following directories:

```
/dev/dsk/cctxdxsx /dev/rdisk/cctxdxsx /oramount ufs 2 yes logging
/dev/dsk/cctxdxsx /dev/rdisk/cctxdxsx /backups ufs 2 yes logging
/dev/dsk/cctxdxsx /dev/rdisk/cctxdxsx /apps ufs 2 yes logging
```

- ☐ Verify permission of /oramount, /backups and /apps directories are 755 before mounting

```
# mount /oramount
# mount /backups
```

```
# mount /apps
```

- Create application directories

```
# cd <path>/drsun/drweb1
```

```
# ./dr.app_dirs
```

The script:

```
creates /oramount/oramaint/[orasoft_polaris,other_polaris] directory
creates /oramount/orabin/dfo-afps/afpspoas directory
creates /oramount/oracle/dfo-afps/afpspoas directory
creates /backups/OAS/afpsppoas directory
untar /usr/local/oracle, /var/opt/oracle, /oramount/oramaint/scripts
creates /oramount/oramaint/[orasoft_pisces,others_pisces] directory
creates /oramount/orabin/oer-commons/crispias directory
creates /oramount/oracle/oer-commons/crispias directory
link /oramount/orabin to /orabin
link /oramount/oracle to /oracle
```

NOTES: The script restores /usr/local/oracle, /var/opt/oracle, /oramount/oramaint/scripts from **polaris**.

The directories /usr/local/oracle, /var/opt/oracle can also be restored from TSM or from tape.

Restore from tape - /var/opt/oracle

```
# mt rewind
Set tape into position:
# mt -f /dev/rmt/0hn fsf 2
# cd /var
# ufsrestore xf /dev/rmt/0hn ./opt/oracle
```

Restore from tape - /usr/local/oracle

```
# mt rewind
Set tape into position:
# mt -f /dev/rmt/0hn fsf 1
# cd /usr
# ufsrestore xf /dev/rmt/0hn ./local/oracle
```

- Create virtual host drcrisp.cit.nih.gov.

```
# cd <path>/drsun/drweb1
```

```
# ifconfig -a (to get the network interface)
```

```
# ./dr.app_vhostnih
```

The script enables virtual host of *drcrisp.cit.nih.gov*

Verify the virtual hosts are up:

```
# ping drcrisp
```

drpuppis: (not for 7/07)

☐ _____ initial

- Create application root directories

```
# mkdir -p /opt/oracle
# chmod 755 /opt/oracle
```

```
# vi /etc/vfstab
Add the disk device for the following directory:
    /opt/oracle
```

- ☐ Verify permission of /opt/oracle directory is 755

```
# mount /opt/oracle
# mkdir /opt/oracle/product
```

7) Update */etc/hosts.allow* file.

- ☐ _____ initial

drandromeda, drandretti, drdanica, drcorvus, drafpsp:

```
% sudo /etc/hosts.allow
```

Do the following:

- Update sshd-fwd-X11 to point the correct address
- Go to the bottom of the file, uncomment all the **sshd:** entries under **DR 7/07** section (if exists)

8) Update */etc/sudoers* file.

drandretti, drdanica: (only)

```
% sudo visudo
```

Go to the bottom of the file and uncomment all the entries under **DR 7/07** section

9) Notify Adrienne that the system up and ready for application restores.

- ☐ _____ initial

Application Restores

Use **ufsrestore** for ufs file system restore and **vxrestore** for *Veritas* file system restore. Two systems that has *Veritas* file systems are *drandretti* and *drdanica*.

To list files on a backup tape:

```
# ufsrestore/vxrestore -ivf /dev/rmt/0hn
```

drandretti (application restore)

drandretti backup tape will contain:

?

1) Restore data from tape to /oraappl directory.

- ☐ _____ initial

Ask for tape 'D/R DRANDRETTI 1' to be mounted (first of two).

Notes: Use *ufsrestore* for the first part of the restore and *vxrestore* for the second part of the restore.

```
# mt -f /dev/rmt/0 rewind
```

```
# cd /
```

```
# ufsrestore x /dev/rmt/0hn (to get the file list back; /var/tmp/dmpfile.a159dru3)
```

```
specify next volume #:" 1
```

```
set owner/mode for '.?' [yn] n
```

```
# vxrestore -x /dev/rmt/0hn
```

(will ask for multiple tapes; the dialog was similar to:)

```
specify next volume #:" 1
```

```
set owner/mode for '.?' [yn] n
```

2) change ownership of restored files to nbsproj:oappdba

☐ _____ initial

```
# chown nbsproj:oappdba /oraappl/od-nbs/backups/drcold/*
```

3) Inform NBS that *drandretti* is restored.

☐ _____ initial

drdanica (application restore)

1) Drdanica dr backup tape will contain:

?

2) Restore data from tape to /oraappl directory.

☐ _____ initial

Ask for tape 'D/R DANICA 1" to be mounted (one of one)

```
# mt -f /dev/rmt/0 rewind
```

```
# cd /
```

```
# ufsrestore x /dev/rmt/0hn (to get the file list back; /var/tmp/dmpfile.s380dru3)
```

```
specify next volume #:" 1
```

```
set owner/mode for '.?' [yn] n
```

```
# vxrestore -x /dev/rmt/0hn
```

(will ask for multiple tapes; the dialog was similar to:)

```
specify next volume #:" 1
```

```
set owner/mode for '.?' [yn] n
```

a. d/*

3) Change ownership of restored files to nbsproj:oappdba/

☐ _____ initial

```
# chown nbsproj:oappdba /oraappl/od-nbs/backups/drcold/*
```

- 4) Inform NBS that *drdanica* is restored.

☐ _____ initial

drandromeda (application restore)

Andromeda backup tape will contain:

/ (root) /usr /var /home
/oraappl/od-nbs/backups

- 1) Restore data from tape to /oraappl directory.

☐ _____ initial

Ask for tape drandromeda or 'andromeda sysbackup' to be mounted

```
# mt -f /dev/rmt/0 rewind
# mt -f /dev/rmt/0hn fsf 4
# cd /oraappl/
# ufsrestore x /dev/rmt/0hn
specify next volume #:" 1
set owner/mode for '.?' [yn] n
```

OR run `mt -f /dev/rmt/0 rewind; ufsrestore xfs /dev/rmt/0hn 4`

- 2) Restore w133prod profile and other special files. These are found in a tar file in /backups/w133prod

☐ _____ initial

```
# mt -f /dev/rmt/0 rewind
# cd /
# ufsrestore -ivf /dev/rmt/0hn
Pick /backups/w133prod to restore
specify next volume #:" 1
set owner/mode for '.?' [yn] n
```

Untar the restored gzip files
`gtar -xvf /backups/w133prod/appl/w133prod.ufiles.tar.gz`

- 3) Inform NBS that drandromeda is restored.

☐ _____ initial

drcorvus (application-restore)

Corvus sysbackup tape will contain:

/ (root) /usr /var /home /usr/local
/oracle/apps/swlib/9ias.90201
/oracle/apps/swlib/9ias.9023.patch

- 1) Restore needed home directories: These files should be restored from the DR CD. If that isn't available for some reason, the TSM or the sysbackup tape can be used.

☐ _____ initial

The following files are needed:

```
/home/eraadmin/.profile
/home/eraadmin/.profilereports
/home/eraadmin/.9023prd_eracommons
/home/eraadmin/VNC/
/home/fitzgers/.profile
/home/mendusch/.profile
```

Verify that the file is there and if not restore from TSM or from corvus sysbackup tape.

TSM: `sudo dsmc restore /home/eraadmin/VNC/`

Tape: Ask for tape “corvus sysbackup” to be Mount tape

```
# mt -f /dev/rmt/0 rewind
# mt -f /dev/rmt/0hn fsf 4
# cd /usr/local
# ufsrestore xf /dev/rmt/0hn ./dr [takes approx 5-10 min]

# /usr/local/dr/siduser.dr -x -s eraadmin -d /usr/local/dr
```

2) Restore data.

☐ _____ initial

Restore the following files:

```
/oracle/apps/swlib/9ias.90201 (sysbackup) [~40 min]
/oracle/apps/swlib/9ias.9023.patch (sysbackup)
```

If the tape “**corvus sysbackup**” is already mounted and was used for the prior step, it is positioned correctly for the next set of restores.

If the tape “corvus sysbackup” was not used for the prior step, ask for tape “corvus sysbackup” to be mounted and issue the next 2 “mt” commands to set tape into position:

```
# mt -f /dev/rmt/0 rewind
# mt -f /dev/rmt/0hn fsf 4
```

Restore data from “corvus sysbackup”:

```
# cd /oracle/apps
(12/06; needed to do “chown eraadmin:eraadmin /oracle”)
# ufsrestore xf /dev/rmt/0hn (for /oracle/apps/swlib/9ias.90201)
# ufsrestore xf /dev/rmt/0hn (for /oracle/apps/swlib/9ias.9023.patch)
```

(could also use “# ufsrestore if /dev/rmt/0hn” to restore files.)

To restore files from TSM:

```
# mkdir -p /oracle/apps/swlib
# dsmc restore -virtualnode=corvus.cit.nih.gov /oracle/apps/swlib/9ias.9023.patch
```

drafpdp (application restore)

Note: the directories below are already restored from CDs (/usr/local/drsun) in *step 6 of **Prepare for Application Restores***.

```
/var/opt/oracle
/usr/local/oracle
/oramount/oramaint/scripts
```

These directories are pulled from *polaris*.

drafpdp (polaris) -

polaris backup tape will contain:

```
/ (root) /usr /var /home
/oramount/oracle
/oramount/orabin/dfo-afps/afpspoas
/oramount/oramaint/orasoft_polaris
/oramount/oramaint/others_polaris
/backups/OAS/afpspoas
```

1) Restore afpdp

Restore from tape - request tape 'polaris sysbackup' unless it was used in a prior step

☐ _____ initial

```
# mt rewind
```

```
Set tape into position:
```

```
# mt -f /dev/rmt/0hn fsf 4
```

```
# cd /oramount
```

```
# ufsrestore xf /dev/rmt/0hn (For /oramount/oracle)
```

```
# ufsrestore xf /dev/rmt/0hn (For /oramount/orabin/dfo-afps/afpspoas)
```

```
# ufsrestore xf /dev/rmt/0hn (For /oramount/oramaint/orasoft_polaris)
```

```
# ufsrestore xf /dev/rmt/0hn (For /oramount/oramaint/others_polaris)
```

```
# cd /backups
```

```
# ufsrestore xf /dev/rmt/0hn (For /backups/OAS/afpspoas)
```

(OR) – Restore from TSM

```
# /usr/bin/dsmc restore -virtualnode=polaris.cit.nih.gov
/oramount/orabin/dfo-afps/afpspoas/
```

```
# /usr/bin/dsmc restore -virtualnode=polaris.cit.nih.gov
/oramount/oracle/dfo-afps/afpspoas/
```

```
# /usr/bin/dsmc restore -virtualnode=polaris.cit.nih.gov
/oramount/oramaint/orasoft_polaris/
```

```
# /usr/bin/dsmc restore -virtualnode=polaris.cit.nih.gov
/oramount/oramaint/others_polaris/
```

```
# /usr/bin/dsmc restore -virtualnode=polaris.cit.nih.gov /backups/IAS/afpspoas
```

drweb1 (application restore)

Note: the directories below are already restored from CDs (/usr/local/drsun) in *step 6 of Prepare for Application Restores*. These directories are pulled from *polaris* and they override the same directories existing on *piscis*.

```
/var/opt/oracle
/usr/local/oracle
/oramount/oramaint/scripts
```

Drafpasp (polaris)

polaris backup tape will contain:

```
/ (root) /usr /var /home
/oramount/oracle
/oramount/orabin/dfo-afps/afpspoas
/oramount/oramaint/orasoft_polaris
/oramount/oramaint/others_polaris /backups/OAS/afpspoas
```

1) Restore afpsp.

☐ _____ initial

Restore from tape - request tape 'polaris sysbackup' unless it was used in a prior step

```
# mt rewind
```

```
Set tape into position:
```

```
# mt -f /dev/rmt/0hn fsf 4
```

```
# cd /oramount
```

```
# ufsrestore xf /dev/rmt/0hn      (For /oramount/oracle)
```

```
# ufsrestore xf /dev/rmt/0hn      (For /oramount/orabin/dfo-afps/afpspoas)
```

```
# ufsrestore xf /dev/rmt/0hn      (For /oramount/oramaint/orasoft_polaris)
```

```
# ufsrestore xf /dev/rmt/0hn      (For /oramount/oramaint/others_polaris)
```

```
# cd /backups
```

```
# ufsrestore xf /dev/rmt/0hn      (For /backups/OAS/afpspoas)
```

(OR) – Restore from TSM

```
# /usr/bin/dsmc restore --virtualnode=polaris.cit.nih.gov
/oramount/orabin/dfo-afps/afpspoas/
```

```
# /usr/bin/dsmc restore --virtualnode=polaris.cit.nih.gov
/oramount/oracle/dfo-afps/afpspoas/
```

```
# /usr/bin/dsmc restore --virtualnode=polaris.cit.nih.gov
/oramount/oramaint/orasoft_polaris/
```

```
# /usr/bin/dsmc restore --virtualnode=polaris.cit.nih.gov
/oramount/oramaint/others_polaris/
```

```
# /usr/bin/dsmc restore --virtualnode=polaris.cit.nih.gov /backups/IAS/afpspoas
```

drcrip (pisces)

pisces backup tape will contain:

/ (root) /usr /var /usr/local /home
/opt /apps/web

pisces appdrbkup tape will contain:

/oramount/oramaint/orasoft_pisces
/oramount/oramaint/others_pisces
/backups/crispias/jweb

1) Restore crisp.

☐ _____ initial

Restore from tape - request for tape 'pisces sysbackup' to be put in the system

```
# mt -f /dev/rmt/0hn rewind
```

```
# cd /oramount
```

```
# ufsrestore xf /dev/rmt/0hn (For /oramount/orabin/oer-commons/crispias)
```

```
# ufsrestore xf /dev/rmt/0hn (For /oramount/oracle/oer-commons/crispias)
```

```
# ufsrestore xf /dev/rmt/0hn (For /oramount/oramaint/orasoft_pisces)
```

```
# ufsrestore xf /dev/rmt/0hn (For /oramount/oramaint/others_pisces)
```

```
# cd /apps
```

```
# ufsrestore xf /dev/rmt/0hn (For /apps/web/N-crisp)
```

(OR) – Restore from TSM

```
# /usr/bin/dsmc restore -virtualnode=pisces.cit.nih.gov  
/oramount/orabin/oer-commons/crispias/
```

```
# /usr/bin/dsmc restore -virtualnode=polaris.cit.nih.gov  
/oramount/oracle/oer-comons/crispias/
```

```
# /usr/bin/dsmc restore -virtualnode=polaris.cit.nih.gov  
/oramount/oramaint/orasoft_pisces/
```

```
# /usr/bin/dsmc restore -virtualnode=polaris.cit.nih.gov  
/oramount/oramaint/others_pisces/
```

```
# /usr/bin/dsmc restore -virtualnode=polaris.cit.nih.gov /apps/web/N-crisp
```

Gather system logs

Gather system logs and copy it over to eosrnde.

Gather system logs and copy it over to eosrnde. This is done at the end of the second test day.

```
% cd <path>/drsund
```

```
% sudo ./dr.collectlogs <path>
```

(e.g. dr.collectlogs /home -or- where space available)

```
% cd <path>
```

(e.g. cd /home)

```
% scp <hostname>_<mon><yr>.tar eosrnde:<path>
```

Where <hostname> = drandromeda, drcorvus, drpavo, drweb1

(e.g. scp drandromeda_Jul06.tar eosrde:/usr/local/drlogs)

Appendix F3 – Windows Restore Procedures

The NIH New Business System recovers two Windows application servers (NBSCOMPUSEARCH and NBSOFTWARE) to support NBS during a disaster situation. Application data is not stored on the servers, but is maintained on a separate database server.

System Backups

Weekly backups of the following application folders/files are made to DVDs and are labeled with the backup date:

NBSCOMPUSEARCH:

D:\oracle
D:\inetpub\wwwroot\prism
D:\software

NBSOFTWARE:

D:*
C:\j2sdk1.4.2_10
C:\ZUD55717

Major security patches are also included in the backup DVDs.

The DVDs are sent to First Federal Corporation, the off-site storage facility where they remain indefinitely.

Restore Procedures

- 1) SunGard support prepares the servers as follows:
 - Load the base operating system and service pack specified by NIH.
 - Configure the computer name and disk partitions specified by NIH.
 - Provide administrative privileges to DCSS DR support staff.
 - Provide remote access to the servers.
- 2) Verify the SunGard setup of the server.
- 3) Configure the IP addresses on the servers to join the server to the NIH network.
- 4) Set up administrative privileges for the following NBS accounts: nbsdba, dogupart, awasthiv, jkarhuri, chunduru, ganesanb, latifias.
- 5) After SunGard support has loaded the DVD, copy the contents of the DVD to the local server drives.
- 6) Inform the NBS customer the servers are ready for them to begin their installation process.

Appendix G – Data Communications

Titan/EOS DR Data Communications Architecture

DCSS has installed a dedicated T1 line between NIH Building 45 and the SunGard recovery center in Wood Dale, IL. The T1 line terminates at a router at each end and is accessible from the NIH network, NIHnet. Firewalls and a switch are connected to the Wood Dale router to provide security protection and segmentation into virtual LANs (VLANs). The Division of Network Systems and Telecommunications (DNST) is responsible for the configuration and management of this network equipment and for contacting the common carrier for any T1 line-related problems. (These telecommunications services are not used for national security emergency preparedness.)

The router in Building 45, and the router, firewalls, and switch in Wood Dale are continuously active and monitored by DNST. The VLAN ports on the Wood Dale switch are set in “shut-down” mode when a disaster recovery is not in progress. Just prior to an NIH disaster recovery test or in the event of a disaster, SunGard personnel must provide the physical connection to the SunGard network, and the VLAN ports must be changed to “no shut-down” mode. When the Wood Dale switch is no longer required, the VLAN ports must be returned to “shut-down”. DNST personnel can change the settings remotely.

The data communications architecture and configurations are described in detail in Attachment 4, *DCSS Firewall Maintenance Activity for December 2005*.

DNST Contact Information

For all support issues, call the DNST Network Operations Center at 301-402-3141 (or 301-506-9069 (pager)).

TCP/IP Subnet Addresses

The following table lists the disaster recovery IP addresses with host names, the associated services supported, and indication of the relationship between disaster recovery IP addresses/host names and NIH Computer Center IP addresses/host names.

The disaster recovery IP addresses/host names are used for the hot site tests. In the event of a true disaster, the domain name service (DNS) on NIHnet needs to be updated to point the production hostnames to the associated disaster recovery IP addresses. Users would then be able to access the disaster systems using either set of host names.

<i>Disaster Recovery IP Address</i>	<i>Disaster Recovery Hostname</i>	<i>Production IP Address</i>	<i>Production Hostname/ User Services/Comments</i>
165.112.213.224/27 VLAN60 (DCSS hosts)			
165.112.213.225	dcss-wooddale-vlan60-e4-pie1.net.nih.gov		
165.112.213.226	dcss-wooddale-vlan60-e4-pie2.net.nih.gov		
165.112.213.227	-- Not defined --		

Disaster Recovery IP Address	Disaster Recovery Hostname	Production IP Address	Production Hostname/ User Services/Comments
165.112.213.228	drtitan2.nih.gov	128.321.64.66	titan2.nih.gov
165.112.213.229	drtitan.nih.gov	128.231.64.34	titan.nih.gov
"	drcd.titan.nih.gov	"	cd.titan.nih.gov / Connect:Direct
"	drftp.titan.nih.gov	"	ftp.titan.nih.gov / FTP
165.112.213.230 through 165.112.213.237	-- Not defined --		
165.112.213.238	drcorvus.cit.nih.gov		eRA
165.112.213.239	drpavo.cit.nih.gov		eRA
165.112.213.240	dreos.cit.nih.gov	Multiple addr	UNIX Alpha Servers
165.112.213.241	drlp.cit.nih.gov	N/A	
165.112.213.242	drweb1.cit.nih.gov	Multiple addr	Web hosts
165.112.213.243	drafpasp.cit.nih.gov		(drweb1 virtual)
165.112.213.244 through 165.112.213.249	-- Not defined --		
165.112.213.250	drcrisp.cit.nih.gov		(drweb1 virtual)
165.112.213.251	drox.cit.nih.gov		TMS
165.112.213.252 through 165.112.213.254	-- Not defined --		
165.112.213.255	(broadcast)		
128.231.164.0/29 VLAN10 (PMS)			
128.231.164.1	dcss-wooddale-vlan10-e2-pie1.net.nih.gov		
128.231.164.2	dcss-wooddale-vlan10-e2-pie2.net.nih.gov		
128.231.164.3	drlapis.cit.nih.gov		lapis.cit.nih.gov
128.231.164.4 through 128.231.164.6	-- Not defined --		
128.231.164.7	(broadcast)		
128.231.164.8/29 VLAN20 (PMS)			
128.231.164.9	dcss-wooddale-vlan20-e2-pie1.net.nih.gov		
128.231.164.10	dcss-wooddale-vlan20-e2-pie2.net.nih.gov		
128.231.164.11	drgarnet.cit.nih.gov		garnet.cit.nih.gov
128.231.164.12 through 128.231.164.14	-- Not defined --		
128.231.164.15	(broadcast)		
128.231.164.16/29 VLAN30 (NBS)			
128.231.164.17	dcss-wooddale-vlan30-e2-pie1.net.nih.gov		
128.231.164.18	dcss-wooddale-vlan30-e2-pie2.net.nih.gov		
128.231.164.19	drcopper.cit.nih.gov		copper.cit.nih.gov

Disaster Recovery IP Address	Disaster Recovery Hostname	Production IP Address	Production Hostname/ User Services/Comments
128.231.164.20 through 128.231.164.22	-- Not defined --		
128.231.164.23	(broadcast)		
128.231.164.24/29 VLAN40 (NBS)			
128.231.164.25	dcss-wooddale-vlan40-e2-pie1.net.nih.gov		
128.231.164.26	dcss-wooddale-vlan40-e2-pie2.net.nih.gov		
128.231.164.27	drandromeda.cit.nih.gov		andromeda.cit.nih.gov
128.231.164.28 through 128.231.164.30	-- Not defined --		
128.231.164.31	(broadcast)		
128.231.164.32/29 VLAN50 (EHRP)			
128.231.164.33	dcss-wooddale-vlan50-e3-pie1.net.nih.gov		
128.231.164.34	dcss-wooddale-vlan50-e3-pie2.net.nih.gov		
128.231.164.35	dr racer.cit.nih.gov		racer.cit.nih.gov
128.231.164.36 through 128.231.164.38	-- Not defined --		
128.231.164.39	(broadcast)		
137.187.54.96/27 VLAN70 (eRA)			
37.187.54.97	dcss-wooddale-vlan70-e5-pie1.net.nih.gov		
37.187.54.98	dcss-wooddale-vlan70-e5-pie2.net.nih.gov		
37.187.54.99	drpiglet.era.nih.gov		
37.187.54.100	drera1.era.nih.gov		
37.187.54.101	drera2.era.nih.gov		
37.187.54.102	dreracluster.era.nih.gov		
37.187.54.103	drerarepsvr.era.nih.gov		
37.187.54.104	drprd.era.nih.gov		
37.187.54.105	droid.era.nih.gov		
37.187.54.106	drapps1.era.nih.gov		
37.187.54.107	drapps2.era.nih.gov		
37.187.54.108	drapps3.era.nih.gov		
37.187.54.109	drapps4.era.nih.gov		
37.187.54.110	drsmeagol.cit.nih.gov		
37.187.54.111 through 37.187.54.126	-- Not defined --		
37.187.54.127	(broadcast)		

Backup Access to the Disaster Site

Access to the hot site will be via SunGard's Web Redirect services over the Internet in the case access via the T1 line becomes inoperable. The IP addresses are assigned at the time of test or disaster; there is no guarantee that they will be the same from one test to another or to a disaster. NATing will occur in the firewalls so that the IP addresses of the hot site host systems remain constant.

Customers will have to be notified of the IP addresses, so they can set their network configurations appropriately in order to communicate to the disaster recovery site.

NIH email Data Communications

DNST has installed redundant high-speed communication links to the NIH Consolidated Co-Location Site (NCCS). The links are connected to NIHnet and terminate in two separate buildings on the NIH campus. If the NCCS site is brought on-line following a Data Center disaster declaration, users can access their email over NIHnet. If, on the other hand, the remote Verizon site is brought on-line, users can access their email over HHSnet which has a dedicated link to the servers located in the Verizon collocation center.

In the event the networks (NIHnet/HHSnet) and/or links are not working, users can access their email over the Internet since both alternate sites have Internet connectivity.

Appendix H – Vendor Contacts

VENDOR	PRODUCT	ADDRESS	SUPPORT CONTACT (phone and email)	REMARKS
ASG	TMON for CICS	1333 Third Avenue South Naples, FL 34102	800-354-3578 support@asg.com 800-932-5536 (headquarters) LSSB contact: Ed Ryan	Site ID: 121000702 www.asg.com
Applied Software, Inc.	SUPERSET	PO Box 566 New Hope PA 18938	215-297-9441 x12 FAX: 215-297-9498 support@appliedsoftware.com LSSB contact: Steve Filbert	Customer ID: DHHS/PHS Attn: Ron Turner ron@appliedsoftware.com www.appliedsoftware.com
BMC Software Inc.	RESOLVE CMF Monitor	1201 City West Blvd Houston, TX 77042	800-537-1813 support@bmc.com LSSB contact: Bill Long	www.bmc.com
Computer Associates International, Inc.	CA-Insight MIA MIM NeuMICS OPS/MVS SMR TMS (CA-1) TSO/MON Vision:Builder	2291 Wood Oak Dr. Herndon, Va. 20171	800-225-5224 (Support Center) 412-494-1341 (MIA;MIM) 703-708-3700 (NeuMICS) 412-494-1302 (OPS/MVS) 856-273-3409 (SMR) 412-494-1324 (TSO/MON) 800-328-7463 (Vision:Builder) LSSB contact (MIA;MIM;SMR): Bobby Bauer LSSB contact (OPS/MVS): Paul Powell LSSB contact (TMS): David O'Brien LSSB contact (NeuMICS;TSO/MON): Steve Filbert	Site ID: 193082 217719 (VISION:Builder) www.ca.com

VENDOR	PRODUCT	ADDRESS	SUPPORT CONTACT (phone and email)	REMARKS
Computer Corporation of America	Model 204	200 West St. 3 rd Floor West Waltham, MA 02451	800-755-4222 LSSB Contact: Hoyt Carelock	Customer ID: NIH www.cca-int.com
Fischer International Systems Corp	IOF	3073 Horseshoe Drive South Naples, FL 34104	1-800-776-7258 support@fischerinternational.com LSSB Contact: Bill Long	Customer ID: FDA www.fischerinternational.com
IBM	CICS DB2	1 New Orchard Rd Armonk, NY 10504-1722	800-426-7378 LSSB Support: Ed Ryan	Customer Number: 9320519 CICS Program No./Entitlement ID: 5697E93/S00T7FK DB2 Program No./Entitlement ID: 5675DB2/ S00SN65 QMF component of DB2 Entitlement ID: S00SN6M www.ibm.com
Innovation Data Processing	FDR/ABR Compaktor FATS/FATAR	275 Paterson Ave Little Falls, NJ 07424	973-890-7300 support@fdrinnovation.com LSSB Contact: Bill Long	Customer ID: USFDA www.innovationdp.fdr.com
Levi, Ray & Shoup	VPS	2401 West Monroe St Springfield, IL 62704	217-793-3800 LSSB Support: Bobby Bauer	Customer ID: MD0027 www.lrs.com
MAX Software, Inc	MAX	3609 S. Wadsworth Blvd Suite 500 Denver, CO 80235	888-376-6629 LSSB Contact: Charles Green	Account Rep: Joe Hassing Phone: ext 103 www.maxsoftware.com
ORACLE Corp	ORACLE	500 Oracle Parkway Redwood Shores, CA 94065	800-223-1711 LSSB Contact: Ed Ryan	Customer ID: 1480 www.oracle.com
Prince Software, Inc	MHtran-2	70 Hilltop Rd Suite 2400 Ramsey, NJ 07446	201-934-0022 800-934-2022 support@princesoftware.com LSSB Contact: ??	www.princesoftware.com
Research Triangle Institute	SUDAAN	P.O. Box 12194 3040 Cornwallis Rd Research Triangle Park, NC 27709-2194	919-541-6000 DCS Contact: Roy Danner	www.rti.org

VENDOR	PRODUCT	ADDRESS	SUPPORT CONTACT (phone and email)	REMARKS
SAS Institute, Inc.	SAS	100 SAS Campus Dr Cary, NC 27513-2414	919-677-8008 LSSB Contact: Angela Bennett	Site ID: 0001233001 www.sas.com
Software Engineering of America, Inc	PDSFAST	1230 Hempstead Turnpike Franklin Square, NY 11010	516-328-7000 800-272-7322 support@seasoft.com LSSB Contact: ??	www.seasoft.com
SPSS, Inc.	SPSS	233 S Wacker Dr 11 th Floor Chicago, IL 60606-6307	312-651-3000 Support: 312-651-3444 support@spss.com LSSB Contact: Angela Bennett	Site ID: 1376 www.spss.com
Sterling Commerce	Connect:Direct	13665 Dulles Technology Dr Suite 130 Herndon, VA 20171-4607	800-299-4031 connect@stercomm.com LSSB Contact: Bobby Bauer	Customer ID: 11653 www.sterlingcommerce.com https://support.sterlingcommerce.com/user/login.asp
GWAC/GSA Schedule	All hardware			www.acqnet.gov - source for acquisition information www.gsa.gov

Appendix I – Contents of the Document Storage Box (Doc Box)

The document storage box is located in the security lab in the Information Security and Awareness Office, Office of the Director, Chief Information Officer, 1040 Fernwood Rd.

The following items are maintained in the doc box:

- Current copy of the *NIH Computer Center Disaster Recovery Plan*, including attachments
- Current copy of the *NIH Computer Center User's Guide (South System)*
- Current copy of the *Titan User's Guide*
- Current copy of the *Titan Batch Processing and Utilities at the NIH Computer Center*
- Current copy of the *Systems Programmers Handbook*
- Current copy of the *Production Systems Quick Reference*
- Current copy of the *EOS Standard Operating Procedures*
- Current copy of the *EOS User's Guide*
- Federal Express shipping labels and envelopes
- Blank floppy disks

Note: The box can be retrieved by calling the IRT hotline at 301-881-9726. The combination to the doc box lock is: 6021

Appendix J – Guidelines for Application Hot Site Tests

(December 17, 2008)

Purpose and Scope

The purpose of this guideline is to provide general instructions to the user community who will be testing their applications at a hot site test (HST). This guideline presents:

- General HST procedures;
- The schedule for the next hot site test;
- General advice on preparing for the HST; and
- Platform specific information for Titan and EOS, including:
 - A brief description of the hot site test environment,
 - Specific instructions for ensuring critical files will be available for the HST,
 - Cautions on potential problem areas with solutions (to ensure the application tests will avoid common mistakes in order to concentrate on truly testing application disaster preparedness), and
 - Procedures to follow on the day of the test.

General information is presented first, followed by two separate subsections covering platform specific information for Titan and EOS testing, respectively.

General Hot Site Test Procedures

The hot site test is scheduled for a three day period with:

- Days one and two dedicated to testing the recovery of the operating environments and recovering the application software and data by the DR support team, and
- Day two being dedicated to customer testing of their recovery operations.

Prior to the HST, the DCSS Disaster Recovery staff determines which backup tapes will be used for the tests. This establishes the *Recovery Point-in-Time*. The Recovery Point-in-Time represents the state of the systems as they existed at the time the backup tapes were made. This Recovery Point-in-Time will lie somewhere between one to two weeks prior to the date of the actual test. All user preparation, including placement of datasets on volumes that are restored at the hot site, must be completed BEFORE this date.

During the tests, in addition to providing customer assistance, the DR staff maintains a running log of the test activities to provide current test status to customers participating in the DR testing and to assist in the post-test reviews.

After every test, debriefings are scheduled to review both the testing of the system and application recovery procedures.

Note Regarding Hot Site System Performance

Be advised that we cannot exactly duplicate production configurations at the disaster recovery hot site. We are limited by the available selection of equipment from the hot site vendor as well as cost considerations. DCSS makes every effort to obtain hot site configurations that best support customer disaster recovery needs, but performance will not always match that of production. **If you experience extremely poor performance during DR testing, please contact us at the time you have the problem, so that we might be able to ascertain where the problem is.** This will help us with planning future modifications to our disaster recovery configurations to provide more effective service.

Connectivity to the Hot Site

IMPORTANT NOTICE: Connectivity to the Hot Site for this test will be over the Internet using SunGard provided IP addresses. This change will require you to update firewall rules to allow connectivity between your site and the Hot Site. SunGard will be providing us the IP ranges one week before the test at which time we will inform you of the IP addresses for the DR host systems.

You should not have to make any changes to your applications since the DR test host names remain the same as prior tests.

December 17, 2008 Hot Site Test Schedule

In order to ensure all application files are backed up on the selected Recovery-Point-in-Time, be sure the application files are stored on the proper volumes/filesystems by close-of-business on the following dates:

Friday, December 5, 2008 – Titan System

Friday, November 28, 2008 - EOS

Monday Dec 15 - System Recovery and Communications Testing (CIT Staff only)
Tuesday Dec 16

9:00 am Monday – On Monday, DR staff will start restoring all Unix operating
8:30 pm Tuesday systems, applications, and databases. On Tuesday, DR staff will
complete the Unix restores, restore all z/OS disks and IPL the
Titan system, and establish and test the data communications links
in preparation for application testing.

As the Unix systems restorations are completed, they will be
turned over to customers to complete their restoration procedures.

Customers do not officially test the applications until the
designated time, but based on past test experience, the systems
may be up and running earlier. Users are welcome to test their
connectivity after the DR staff has announced that you may do so.

The systems will remain up overnight, and users may perform testing if desired, but CIT staff will not be available to resolve any problems until the official customer test time.

Wednesday Dec 17

Application Testing

8:00 am – 4:00 pm

Titan and EOS DR systems are available for testing applications.

4:00 pm - 1:00 am

Customers may continue testing, but be advised there will be no full CIT staff support to help resolve problems.

Test Support Contact Information, Wednesday Dec 17, 8:00 am - 4:00 pm

Titan Support: (301) 496-5181

Provide your name and contact phone number and state you are calling for “Disaster Recovery Support”. We will take your information and have the appropriate support person contact you within five minutes.

Unix Support: Submit an EXPEDITED ASR that clearly states it is a DR test request.

Alternately, you may call (301) 496-9160. Provide your name and contact phone number, identify which DR system you are using (e.g., EOS, NBS, etc.) and state you are calling for “Disaster Recovery Support”. We will take your information and have the appropriate support person contact you within five minutes.

Web site information: dr.cit.nih.gov

On the days of the test, a Web site will be available with a posting of the status of the recovery process and other useful information. Customers can check this Web site for updates indicating hot site systems’ availability.

General Contact Information

Please contact Adrienne Yang, Disaster Recovery Coordinator, at (301) 496-1053 with any questions or concerns.

Next Scheduled Test Date: Tuesday, July 14, 2008

Preparing for the Hot Site Test

Ensure All Critical Files will be Available – Maintain a **complete** list of **all** files required for processing the application in recovery mode after a disaster. If the application uses cataloged procedures or Job Control Language on the mainframe, or *cron* jobs on EOS, review each of them to identify all files needed to successfully execute the procedures/jobs. Also, review all command procedures/script files that may reference files that are created, used, or updated. Reference the platform specific sections for further instructions for ensuring the availability of critical files for testing.

Use the Password that was in Use Prior to the Recovery Point-in-Time Date for the System – All system and user passwords reflect the password in use at the point-in-time the system backup tapes were made. Therefore, users who will be participating in the application HST must be sure to use the password that was in effect prior to the date of the system backup (listed above). This is particularly critical for those users who have changed their passwords between the time of the system backup and the date of the HST.

Ensure Firewalls are Configured to Allow Communication with the Hot Site – Update firewalls with the following disaster recovery IP addresses/hostnames, as appropriate:

<i>Disaster Recovery IP Address</i>	<i>Disaster Recovery Hostname</i>	<i>Production IP Address</i>	<i>Production Hostname</i>	<i>CIT Enterprise User Services</i>
To be determined	drtitan2.nih.gov	128.321.64.66	titan2.nih.gov	
To be determined	drtitan.nih.gov	128.231.64.34	titan.nih.gov	
To be determined	drcd.titan.nih.gov	"	cd.titan.nih.gov	Connect:Direct
To be determined	drftp.titan.nih.gov	"	ftp.titan.nih.gov	FTP
To be determined	drcorvus.cit.nih.gov			eRA
To be determined	dreos.cit.nih.gov	Multiple addresses		UNIX Alpha Servers
To be determined	drweb1.cit.nih.gov	Multiple addresses		DR Web host
To be determined	drlapis.cit.nih.gov	Multiple addresses		PMS
To be determined	drgarnet.cit.nih.gov			PMS
To be determined	To be determined			NBS
To be determined	drracer.cit.nih.gov			EHRP

Ensure Connect:Direct Procedures Use the Correct snode – If you use the *host name* to specify the system (snode=<hostname>) to which you are connecting, you will have to change it for the hot site test before you can run C:D. The following table lists the DR host names to use.

<i>Disaster Recovery Host Name</i>	<i>Production Host Name</i>
drcd.titan.nih.gov	cd.titan.nih.gov
dreos.cit.nih.gov	eos.cit.nih.gov
drgarnet.cit.nih.gov	garnet.cit.nih.gov

If you use the *node name* to specify the system to which you are connecting you don't have to make any changes.

We highly recommend that if you are using host name, you change your procedures to specify node name. The following table lists the node names:

<i>System</i>	<i>Node Name</i>
Titan	nih.std.ndm
eos	eos.ndm
garnet	garnet.ndm

The following is an example of a Connect:Direct process (for UNIX) using the node name to specify the Connect:Direct node to which you are connecting:

```

tocu process snode=nih.std.ndm snodeid=(uuu,ppppppp)
  copy from (file=testcd)
    to (file=uid.filename
      disp=rpl)
  pend

```

Titan System HST

Titan System Hot Site Test Environment

The Data Center's DR program is designed to support only a subset of the full production version of the z/OS operating environments for Titan. The objective of the DR program is to support only the essential operations and functions of application participating in the disaster recovery program. The following is the hot site system environment for Titan:

DASD – All essential system volumes, data base volumes, private volumes designated by an application, special disaster recovery volumes, DISR01, DIST00, DIST01, and DIST02, and **all** public volumes will be restored.

Tapes - None of the tapes from the Titan system production tape library will be taken to the hot site for HSTs. Copies of the Titan system backup tapes are sent to restore the Titan system at the hot site. Any tapes that are required to run the applications should remain at the Data Center. Only copies should be used for the hot site tests. Some scratch tapes will be available at the hot site and may be temporarily assigned to users during the HST exercises.

NJE - NJE services are not part of the Center's DR system, but depending on customer needs, these services may be available during future HSTs.

Printing from the Hot Site - The most reliable method for obtaining printed output from a disaster test is to print it on a network attached printer in your office using the VPS facility. Any output not printed before the end of the test will be purged.

File Transfers – Files may be transferred to/from the DR system using the file transfer protocol (FTP). To perform an FTP, logon to drftp.titan.nih.gov.

Post-Test Examination of Test Results - FTP and VPS printing provide you two methods for saving test data to examine at your leisure following a test.

Connectivity – The only connectivity will be via TCP/IP. Only the TCP/IP connections to Connect:Direct will be available.

Ensuring Critical Files are Available for the HST

Prepare backup and restore procedures for files that are not included in standard Titan system backup procedures. If you have tapes to be sent to the hot site for your test, you will be notified when to send them to the Data Center for shipment.

Ensuring User Profiles Will be Restored at the Hot Site

Since all public volumes are restored, all user profiles should also have been restored for the test. If for some reason this was not the case for previous tests, prior to the hot site test Recovery-

Point-in-Time, log onto the Titan production system, and move the affected profiles and data sets to a volume that is restored at the hot site, either a non-public volume that is restored for the application, or any of the disaster recovery volumes – DISR01, DIST00, DIST01, DIST02. The ISPF profile uses either of the following naming conventions: \$iii.ISPF.ISPPROF or aaaaiii.ISPF.ISPPROF, and the WYLBUR profile uses the following naming convention: aaaaiii.@WYLBUR.PROFILE, where “\$iii” is the userid and “aaaaiii” is the account/initials.

Examine each data set referenced in member TSLOGON (if this member exists in your ISPF profile) and in your WYLBUR profile to ensure they are not stored on a public volume. Any data set on a volume beginning with “PUB”, “DS”, or “MIGRAT”, is located on a public volume.

Once moved, you should not need to move the profiles and data sets again.

A Rexx exec, DRMOVE, can be used to move the ISPF profile dataset to DIST01. Before executing the exec, exit ISPF. The exec can be used to move your profiles or other user’s profiles for which you have the proper RACF authorities. From the ready prompt enter DRMOVE. You will be prompted to either hit the Enter key to move your profile dataset or enter a userid for the profile that is to be moved. The exec only allows you to move the profile for one user at a time.

NOTE: This command only moves the profile dataset; referenced datasets will have to be moved using standard commands.

There are numerous methods for moving data sets, but the following process should work for both sequential and partitioned (PDS) data sets. Assuming the ISPF profile, \$iii.ISPF.ISPPROF, is to be moved to DIST01, from the TSO READY prompt, enter the commands:

```
COPY ISPF.ISPPROF ISPF.ISPPROF.NEW VOLUME(DIST01) UNIT(3390)
RENAME ISPF.ISPPROF ISPF.ISPPROF.OLD
RENAME '$iii.ISPF.ISPPROF.NEW' '$iii.ISPF.ISPPROF'
```

Repeat the above process for all data sets referenced in the profile.

Log on to verify that the new profile works correctly. Delete the old ISPF profile with the command (from the TSO READY prompt again):

```
DELETE ISPF.ISPPROF.OLD
```

On the Day of the Hot Site Test

The hot site system will be ready for testing beginning at 8:00 am, Eastern time on the day scheduled for application testing. It should be noted, the Data Center production systems will continue to be available to users during regular business hours on that day. During testing, an easy way to distinguish the two systems is to think of the NIH production system as the *home* system and the hot site system as the *away* system. Any processing occurring on the away system does not affect the applications and processing running on the home system.

Logging In

CIT has installed a T1 line from the NIH campus to the vendor hot site. The NIH terminus of the T1 line is located in another building on the NIH campus, separate from the Data Center. The T1 line is accessible from the NIH network, NIHnet.

If on the day of the test, there are problems with this connection, an Internet connection will be used instead and users will be notified.

To connect to the Titan hot site system:

- For TN3270, use the hostname: drtn3270.titan.nih.gov
- For FTP, use the hostname: drftp.titan.nih.gov

At the LOGON screen type the same logon string normally used to access the NIH Titan production facility.

Potential Problems That May Be Encountered During the HST

Based on experiences from past HST exercises, the following are common problems, with recommended solutions, that may possibly occur during hot site testing.

Problem	Solution
<i>Error encountered when logging on</i> (because your profile and/or referenced files are stored on a volume that has not been restored; you are placed at the TSO Ready prompt instead of ISPF)	Issue the following command at the Ready prompt: DEL ISPF.ISPPROF NSCR Log off and then log on again. The system will automatically build a new default profile for you on the DR system. Note that the new profile contains only standard settings; it will not contain any non-default settings that you may have in your production system profile.
<i>System catalog conflict</i> (because the referenced data set is on a volume that was not restored)	Issue the following TSO command to delete a catalog entry for a non-existent data set on the DR system: DEL data-set-name NSCR Note: Executing this command on the DR system will <u>not</u> affect data sets on the NIH production system.
<i>Cannot submit jobs</i> (you get an error message like “unable to allocate temporary data set”)	Using panel 3.4, uncatalog your SYS4.SPFLOG1.LIST data set.

Problem	Solution														
<i>Job is not processing</i>	<p>The User Display Facility (UDF) allows you to display information about jobs processed by ThruPut Manager. UDF is invoked through the ISPF command TMUSER. You can assign TMUSER to a PF key. To use UDF:</p> <ol style="list-style-type: none"> 1. Invoke UDF in IOF using one of two methods: <ul style="list-style-type: none"> • Place the cursor at the job name and press the PF key you have assigned to TMUSER. or • Enter the TMUSER command on the ISPF command line, move the cursor to the job name, and press Enter. <p>You will see one or more Information Summary Lines. For example:</p> <pre>GL3005TB(J01143) _ JB JC JL H</pre> <p>The Information Summary Line contains the job name and job number. It may also contain a command line and one or more acronyms indicating the ThruPut Manager services affecting the job. The most common acronyms are:</p> <table border="1" data-bbox="699 1031 1336 1297"> <tr><td>DC</td><td>Dataset Contention Services</td></tr> <tr><td>JB</td><td>Job Binding Services</td></tr> <tr><td>JC</td><td>Job Chaining Services</td></tr> <tr><td>JL</td><td>Job Limiting Services</td></tr> <tr><td>JS</td><td>Job Setup Services</td></tr> <tr><td>MH</td><td>Multi-Hold Services</td></tr> <tr><td>RS</td><td>Robotic Setup Services</td></tr> </table> <p>Highlighted acronyms indicate that the service is causing the job to be held.</p> <p>The line may also contain the letters H or D, showing whether the job has been held or deferred by ThruPut Manager.</p> 2. To see more information about an acronym, place the cursor under the acronym and press Enter. 3. You can enter the following commands on the command line: <ul style="list-style-type: none"> • D to see job details • V to see which volumes are used 	DC	Dataset Contention Services	JB	Job Binding Services	JC	Job Chaining Services	JL	Job Limiting Services	JS	Job Setup Services	MH	Multi-Hold Services	RS	Robotic Setup Services
DC	Dataset Contention Services														
JB	Job Binding Services														
JC	Job Chaining Services														
JL	Job Limiting Services														
JS	Job Setup Services														
MH	Multi-Hold Services														
RS	Robotic Setup Services														

Problem	Solution
<p>Job fails (because the referenced data set was not restored)</p>	<p>The process discussed below may be used at the hot site to restore your data set from one of the FDR/ABR full volume dump tapes sent to the hot site.</p> <p><u>Preparation</u></p> <p>You will need the following information:</p> <ul style="list-style-type: none"> • The full name of the data set to be restored • The volume the data set was on (available from the ISPF screen 3.4) <p><u>Using the FDR Primary Options Menu</u></p> <ol style="list-style-type: none"> 1. On the ISPF Primary Option Menu, select option C. 2. On the Additional Products menu, select option A. <p>The FDR Primary Options Menu is displayed.</p> <p><u>Creating Job Statements</u></p> <p>If this is the first time you have used FDR to restore a data set, you must create job statements for the print request and the restore request. If you have previously restored a data set, you can skip this section.</p> <ol style="list-style-type: none"> 1. On the FDR Primary Options Menu, select option J. 2. Modify the two sample job statements for your jobs. 3. Press PF3 to return to the FDR Primary Options Menu. <p><u>Determining the Backup Generation Number</u></p> <p>In order to do the restore you will need to know the generation number of the backup.</p> <p>There are two methods to do this.</p> <p><i>The first method:</i></p> <ol style="list-style-type: none"> 1. On the FDR PRIMARY OPTIONS MENU, select option 1 (reports). 2. On the FDRABR REPORT PANEL, enter option 2, the dataset name, and the original disk volume that it was on, and then hit enter.

Problem	Solution																		
	<p>3. This should produce one or more screens of output. Look for lines of the following format:</p> <p>BKD(00)-2004.206 SFX-C1004200 FN-0040 VOLS-E00427</p> <p>Each such line of output represents one backup of the disk containing your dataset. Only one set of backups will be available at the disaster site, so you need to identify which backup is available. To do this, examine the day of year of the backup (206 in the example). You need to find the line of output which has a day of year equal to a date falling on the weekend that the point in time backups were taken.</p> <p>Now examine the string of characters following 'SFX-' (C1004200 in the example line). The 3rd through the 6th characters in the string (0042 in the example line) is the backup generation number. You will need to know it in order to restore your dataset.</p> <p><i>The second method:</i></p> <p>If you have trouble determining the backup day of year or the backup generation number, call the DR User Support Team. You will be contacted by a member of the DR restore team, who should be able to tell you the backup generation number for your disk from their listings of the backups.</p> <p><u>Restoring a Data Set</u></p> <ol style="list-style-type: none"> 1. On the FDR Primary Options Menu, select option 2. 2. On the FDRABR Restore Panel enter the following information: <table border="1" data-bbox="667 1436 1435 1776"> <thead> <tr> <th>OPTION</th><th>Data To Enter</th></tr> </thead> <tbody> <tr> <td>SELECT OPTION</td><td>B</td></tr> <tr> <td>COPY OPTION</td><td>2</td></tr> <tr> <td>PROCESS OPTION</td><td>B</td></tr> <tr> <td>GENERATION</td><td>the generation number</td></tr> <tr> <td>CYCLE</td><td>0</td></tr> <tr> <td>ORIGINAL VOLUME</td><td>volume serial number for</td></tr> <tr> <td>NEW VOLUME SERIAL</td><td>DSP101</td></tr> <tr> <td>OTHER</td><td>original data set name</td></tr> </tbody> </table>	OPTION	Data To Enter	SELECT OPTION	B	COPY OPTION	2	PROCESS OPTION	B	GENERATION	the generation number	CYCLE	0	ORIGINAL VOLUME	volume serial number for	NEW VOLUME SERIAL	DSP101	OTHER	original data set name
OPTION	Data To Enter																		
SELECT OPTION	B																		
COPY OPTION	2																		
PROCESS OPTION	B																		
GENERATION	the generation number																		
CYCLE	0																		
ORIGINAL VOLUME	volume serial number for																		
NEW VOLUME SERIAL	DSP101																		
OTHER	original data set name																		

Problem	Solution				
	<table border="1" data-bbox="667 226 1435 306"> <tr> <td data-bbox="667 226 1040 262">DSNAME/FILTER</td><td data-bbox="1040 226 1435 262"></td></tr> <tr> <td data-bbox="667 262 1040 306">OTHER NEW NAME</td><td data-bbox="1040 262 1435 306">new data set name</td></tr> </table> <p data-bbox="618 344 1419 411">You may need to scroll down to see the OTHER NEW NAME field.</p> <p data-bbox="570 420 1305 487">3. Press Enter. The data set will be restored to the new data set name.</p> <p data-bbox="570 527 1382 562"><u>Cataloging the Restored Data Set Under the Original Name</u></p> <p data-bbox="570 602 1435 745">After the data set is restored, you will probably want to change the new data set name to the original data set name. You must first uncatalog the original data set because it is still listed in the catalog even though the data set does not exist.</p> <ol data-bbox="570 785 1406 999" style="list-style-type: none"> 1. Use the ISPF screen 3.4 to list the data set. 2. Enter the UNCATALOG line command in the command area next to the original data set name. 3. Enter the RENAME line command in the command area next to the new data set name. 4. Rename the data set to the original name. 	DSNAME/FILTER		OTHER NEW NAME	new data set name
DSNAME/FILTER					
OTHER NEW NAME	new data set name				
<i>Output from DR Titan won't print via VPS to your network printer</i>	Have your firewall group permit LPR traffic from 165.112.213.229 to enter your network.				
<i>Have accessed the Titan home system when intended to access the Titan hot site system</i>	<p data-bbox="570 1157 1073 1184">To connect to the Titan hot site system:</p> <ul data-bbox="570 1192 1312 1266" style="list-style-type: none"> • For TN3270, use the hostname: drtn3270.titan.nih.gov • For FTP, use the hostname: drftp.titan.nih.gov 				
<i>Denial of access to a tape</i> (because the tape was created after the Recovery-Point-in-Time; the assignment to the user/application is not recorded in the tape library system at the hot site.)	Treat the tape as a foreign tape at the hot site by adding EXPDT = 98000 to the DD card.				

EOS Hot Site Test

EOS Hot Site Test Environment

The Data Center's DR program is designed to support only a subset of the full production version of the EOS operating environments. The objective of the DR program is to support only the essential operations and functions of applications participating in the disaster recovery program.

DCSS has contracted for multiple ALPHA and Sun servers to host the participating applications. These servers will be configured with the current versions of the Alpha Tru64 UNIX and Solaris operating systems, and Oracle database.

The hot site server configurations have sufficient memory and disk space to accommodate the execution of the applications. All application and database files that have been identified by the application owner as being required, will be restored to the hot site servers.

Ensuring Critical Files are Available for the HST

Prior to the hot site test, DCSS will request the list of data that is to be backed up for the test.

NOTE: To ensure an efficient and error-free restoration of your files, include only those files necessary for application processing, e.g., application files, database files, configuration files. Do not include old log files, report files, or other files that can easily be recreated.

Accounts on the Hot Site ALPHA Server

Prior to the HST, DCSS will request the names and IP addresses of all users who will be logging on directly to the hot site ALPHA Server. DCSS will set up accounts on the hot site host for the test and will notify the testers of the login IDs and passwords.

Considerations for Oracle

In order to minimize the possibility of inadvertently connecting to the wrong databases while performing DR testing, the following are suggestions to consider:

For client (remote) machines connecting to the DR Oracle databases:

- Ensure that the sqlnet.ora file is removed or the references to production Oracle Names Servers are removed.
- Ensure that tnsnames.ora entries that will be used for testing are modified. Either add a new database alias (e.g., that starts with DR), or modify the existing database alias definition to point to the DR host. See the section heading, Connecting to a Disaster Recovery Database Instance, below for further instructions on this.

For host (local) DR database machines:

- Determine whether you want to have any database alias definitions removed or changed.
- If using database links or specifying aliases during connection that use aliases, request that the database tnsnames.ora file be changed to point to the appropriate databases (e.g., host, sid, port).
- If testing using database links, either request a change to the database alias in the host tnsnames.ora file, or, if the database links were created with host name parameter or password in the using clause, recreate the link.
- If appropriate, alter database users to use a non-production password.

Client changes for DR Oracle Application Server:

- Modify any hard coded URL's pointing to the production database within the application to point to the DR site.
- For 9iAS Release 2, customers will need to configure DAD's to point to the DR database, after CIT Oracle System staff install and configure the middle tier software to point to the DR database.
- For 9iAS Release 1, if customers want the database alias changed on the middle tier machine, the DAD's will need to be modified to point to the DR database alias, after CIT System staff has restored and configured the middle tier software to point to the DR database.

The following changes will be made by CIT Oracle System staff on the DR machines.

For the DR Oracle Database instances:

- Modify the host name in listener.ora file to point to DR host.
- Remove the sqlnet.ora entries pointing to the production Oracle Names Servers.
- Verify with customers regarding preferred changes they want to the DR database local tnsnames.ora file.
- Verify customers want the database alias changed in addition to the host value.
- Verify with customers regarding the removal or modification of additional database aliases in the tnsnames.ora file.

For the DR Oracle Middle Tier instances:

- Modify the tnsnames.ora file to specify the DR host for the database alias in \$IASHOME and \$6iSERVER_HOME.
- Modify the httpd.conf file to specify the DR virtual host.
- If URL Redirection is used, make sure it is pointing to DR site.
- Modify the httpd.conf file to have the LISTEN parameter pointing to the virtual IP address of the DR site.
- Modify the oem.conf file to have the virtual host parameter pointing to DR site.
- If Report Server is used, set the DISPLAY parameter point to IP address of the DR host.

On the Day of the Hot Site Test

The hot site system will be ready for testing beginning at 8:00 am, Eastern time on the day scheduled for application testing. It should be noted, the Data Center production systems will continue to be available to users during regular business hours on that day. During testing, an easy way to distinguish the two systems is to think of the NIH production system as the *home* system and the hot site system as the *away* system. Any processing occurring on the away system does not affect the applications and processing running on the home system.

Hot Site Hostname

CIT has installed a T1 line from the NIH campus to the vendor hot site. The NIH terminus of the T1 line is located in another building on the NIH campus, separate from the Data Center. The T1 line is accessible from the NIH network, NIHnet.

If on the day of the test, there are problems with this connection, an Internet connection will be used instead and users will be notified.

You will use a special hostname for the DR test. The DR hostname has been constructed by putting “dr” at the beginning of your production hostname. For example: **dreos.cit.nih.gov** is the DR hostname for eos.cit.nih.gov.

Logging In

Direct logins use *ssh*.

Connecting to a Disaster Recovery Database Instance

If you will be using SSH to connect to your Disaster Recovery instance, you do not have to take any special steps. The tnsnames.ora file on the dreos.nih.gov machine will be updated for your instance.

If you will be using a client/server connection, you can do either of the following:

- 1) Change the host parameter in the tnsnames.ora file on your client machine for the alias you will be using for the disaster recovery test. Change the statement:

HOST = <hostname>

to

HOST = dreos.cit.nih.gov

The entry should resemble the example in 2) below:

- 2) Create a new alias “drtest” in the tnsnames.ora file to be used for disaster recovery testing:

```
drtest =
(DESCRIPTION =
(ADDRESS = (PROTOCOL = TCP)(HOST = dreos.cit.nih.gov)(PORT = <port number>))
(CONNECT_DATA = (SID = test))
)
```

Potential Problems That May Be Encountered during the HST

Based on experiences from past HST exercises, the following are common problems, with recommended solutions, that may possibly occur during hot site testing.

Problem	Solution
<i>Error encountered when logging onto a DR server</i> (because you entered the incorrect password)	If you are logging onto a Sun server, you will have to use the initial default password for your account. If you are logging onto a Tru64 or HP-UX server, and you changed your password after the date the system backup tapes were created, use your prior password.
<i>You get a warning message about the certificate when accessing the Web site</i> (because the certificate is associated with the production Web site rather than the DR Web site)	You can safely hit OK to continue.

Appendix K – Mainframe Communications

Local Terminals

Terminal access to the DR Titan systems from the Herndon site is via SunGard supplied PC's attached to a Visara server. Visara supplies both local SNA terminal and console support. All 32 LUs, except the consoles, need to be defined to VTAM. See member DRLOCALS in the VTAM start configuration. Although the PC's are using TCP/IP to communicate to the Visara server, they are on a closed network with no access beyond the Visara server.

Once DRLOCALS has been activated, the cursor should move down 2 lines from the upper left corner. Logon is accomplished using:

LOGON APPLID(TSO) (Also TSO4 or TSO9)

Communication between SYS4 and SYS9 at DR

There are two physical paths providing communications between the LPARs, a CTC connection and a LAN connection. The CTC has two logical paths, TGN=21 and TGN=10; the LAN has one, TGN=8.

When VTAM is started, it will attempt to establish an XCF connection due to the XCFINIT=YES start parm. This will be TGN=21. Members DR*CTC and DR*AHHC will bring up another path using the CTC, TGN=10. Members EEXCA and DR*EESW will bring up an Enterprise Extender connection across the LAN, TGN=8. (All of these members are in the VTAM start configuration.)

TGN=10 is the preferred communication path.

The TCP/IP LAN connection provides the ability to use FTP, etc. between the LPARs.

Communications to NIH

A dedicated T1 line between the NIH campus and the Wood Dale Recovery Center provides NIHnet connectivity to the hot site. See Appendix G for details. This IP connection allows an Enterprise Extender link to be established between Titan at the hot site and the NIH production system. Members EEXCA and DREENIH will establish this connection.

Since this is an IP connection, FTP, etc may be used between the MVS systems at NIH and DR.

Start up commands and JCL

The following are listed here for reference only. See Appendix F1 for details. If you bounce VTAM for any reason, you will need to issue these commands at a minimum.

- 1) S NET,,(LIST=DR)

- 2) S TCAS
- 3) S TCPIP
- 4) S EMSPROC (Netview Access Services)

Establishing sessions to NIH

During tests, the Enterprise Extender connection allows establishment of interactive and batch connections from DRTITAN to NIH production Titan. TSO sessions from DR to NIH may be established using LOGON APPLID(NIH.TSO4). Batch work is transmitted between systems via an NJE connection.

Make sure the cdrsc for NIHJES2 is available in order to bring up the NJE connection on DRTITAN. This is in member DRCDRSCS. The JES2 applid must also be available; it is in member DRJES2. Both of these are in the VTAM start configuration.

Issue:

\$SLGN1
\$SN,A=NIHJES2

Connect:Direct

See Appendix F1 for the procedures to obtain keys.

Connect:Direct is started at the DR using the same netmap as on SYS4. The Unix machines that send files to Titan will have different addresses, but because NETMAP.CHECK=NO is coded in the start parms, changes to the netmap are not needed.

JCL and member locations

The started tasks are stored in SYS1.SYSn.PROCLIB. The VTAM members are in NIH.VTAMLSTn

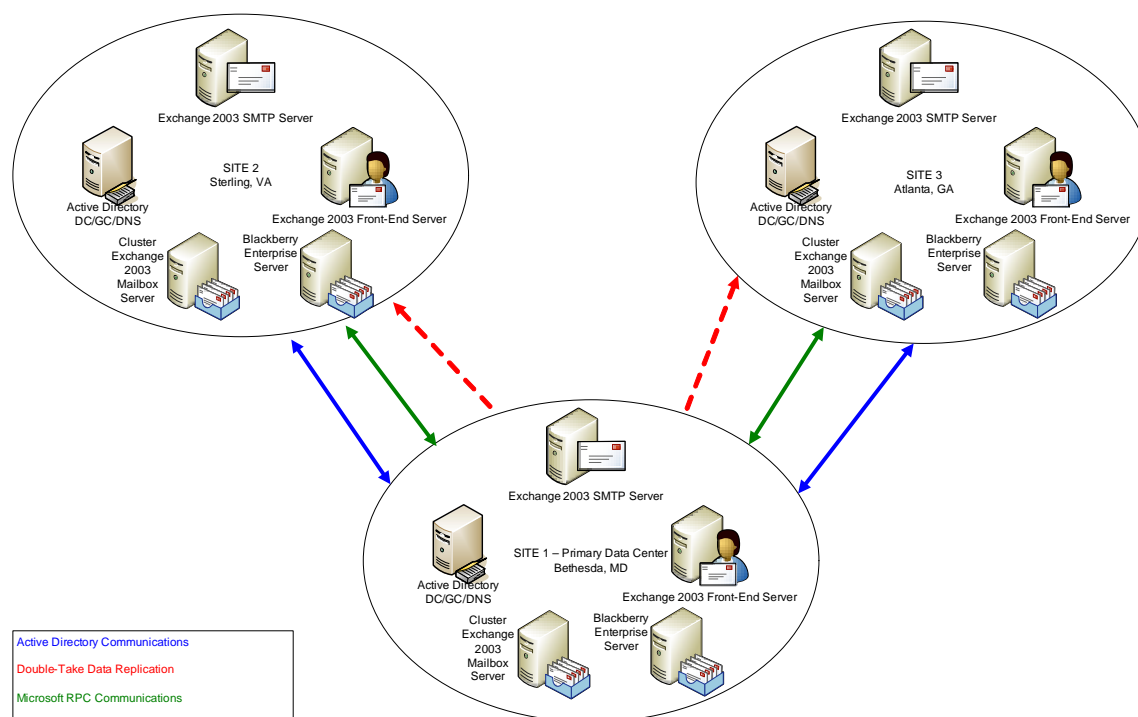
Appendix L – NIH Electronic Messaging Recovery

NIH CES Messaging DR/HA Design and Configuration

The Central Email Service has deployed a High-Availability/Disaster Recovery Solution incorporating Microsoft Windows Server 2003 Server Clusters and Host-Based Asynchronous replication software. The goals of the design are to:

- Provide service for 5000 mailboxes
- Have customers login to those mailboxes using their existing username and password
- Be able to send and receive e-mail to/from their existing SMTP addresses
- Have the solution be online and ready for customer access in 1 hour or less

Using Clustering and host-based replication of data, we have met and exceeded those goals by also providing customers with their complete mailbox data.



In the event the primary data center is declared a disaster site, and messaging services cannot be delivered from the primary data center, management will initiate failover. Customers who migrate to the DR/HA platform will be able to access their e-mail accounts within the following 60 minutes via OWA at the <https://mail.nih.gov>. Depending on the severity of the disaster, management will direct actions to address messaging services for the remainder of the NIH staff.

The following sections of this document outline the specific technical configurations and procedures for executing failover and failback.

Primary Data Center Cluster Configuration

Two (2) MSCS Server Clusters on Windows Server 2003 SP2 Enterprise Edition. Each is an Exchange Server 2003 SP2 Enterprise Edition Mailbox Server two-node Active/Passive Cluster. Each cluster consists of two cluster groups, the **NIHCESCLUSTERx Default Cluster Group**, and the Exchange Virtual Server group, **CES-EVS-x**. Each cluster node has two network cards installed, one for **PUBLIC NETWORK** communications, and one for **PRIVATE CLUSTER** communications.

The **PRIVATE** network is used solely for cluster communications, such as the cluster heartbeat, quorum updates, etc. The **PRIVATE** NIC is connected to an Internal Ethernet switch that does NOT connect back to NIHNet.

The **PUBLIC** network is used by all clients to communicate with the server resources. It's NIC is connected to NIHNet, on the Messaging VLAN.

Each Server Node has at least four (4) IP addresses:

- Physical node IP address
- Private Network IP Address
- Cluster IP Address
- Exchange Virtual Server IP Address

All resources in a cluster group can only be owned or active on one node at a time. In the event of a problem with that node, the cluster service will move those resources to the other node automatically. The cluster service owns and manages all cluster resources, so any changes that need to be made to those resources should be done using the Cluster Admin utility (i.e. – To stop the SMTP Service, you use the Cluster Admin utility to take the Exchange SMTP Virtual Server Instance 1 offline)

➤ **NIHCESMLBXHA (Exchange Virtual Server)**

- NIHCESMLBXHA1A – Physical Server Node (156.40.71.140)
- NIHCESMLBXHA1B – Physical Server Node (156.40.71.141)
 - **NIHCESCLUSTER1 Default Cluster Group** – Defines the cluster object, and contains the following resources:
 - ◆ Disk Q: (Quorum) – Cluster object Physical Disk resource; used as the Quorum disk, storing the definitive copy of the cluster configuration so that regardless of failures, the cluster configuration remains consistent – No dependencies
 - ◆ Cluster IP Address (156.40.71.142) – Cluster object IP Address Resource; used by the cluster service and cluster management utilities to manage the cluster groups and resources – no dependencies

- ◆ Cluster Name (NIHCESCLUSTER1) – Cluster object NetBIOS Resource; used by the cluster service and cluster management utilities to manage the cluster groups and resources – **Dependent on the Cluster IP Address Resource**
- ◆ Distributed Transaction Coordinator – Cluster object MS-DTC resource; required by Exchange Server 2003 clusters, but should be owned by the default cluster group, not the Exchange Virtual Server – **Dependent on the Quorum Disk, IP Address, and Network Name resources**
- **CES-EVS-1** – Exchange Virtual Server, contains the following Resources:
 - ◆ Exchange SG1 LOGS Disk G: - Physical Disk Resource; Location of SG1 Log Files – No Dependencies
 - ◆ Exchange SG2 LOGS Disk H: - Physical Disk Resource; Location of SG2 Log Files – No Dependencies
 - ◆ Exchange SG3 LOGS Disk I: - Physical Disk Resource; Location of SG3 Log Files – No Dependencies
 - ◆ Exchange SG4 LOGS Disk J: - Physical Disk Resource; Location of SG4 Log Files – No Dependencies
 - ◆ Exchange MTA/SMTP Disk N: - Physical Disk Resource; Location of MTA and SMTP Virtual Server Queue Directories – No Dependencies
 - ◆ Exchange SG1 DATA Disk R: - Physical Disk Resource; Location of SG1 Database Files – No Dependencies
 - ◆ Exchange SG2 DATA Disk S: - Physical Disk Resource; Location of SG2 Database Files – No Dependencies
 - ◆ Exchange SG3 DATA Disk T: - Physical Disk Resource; Location of SG3 Database Files – No Dependencies
 - ◆ Exchange SG4 DATA Disk U: - Physical Disk Resource; Location of SG4 Database Files – No Dependencies
 - ◆ Exchange IP Address (156.40.71.143) – IP Address Resource of the Exchange Virtual Server; registered on the **PUBLIC** interface – No Dependencies
 - ◆ Exchange Network Name (NIHCESMLBXHA) – NetBIOS Network Name Resource; this resource represents the Exchange Server listed in the Exchange System Manager, and is the Exchange Server name clients connect to, it is bound to the Exchange IP Address and must register in DNS in order for the cluster service to bring it online – **Dependent on the Exchange Network Name Resource**
 - ◆ Exchange System Attendant – Exchange System Attendant Resource; bound to the **Exchange Network Name** resource; represents the Exchange System Attendant Service for the Exchange Virtual Server – **Dependent on Exchange Network Name Resource and ALL Physical Disk Resources**
 - ◆ Exchange Information Store Instance – Information Store Resource; represents the Information Store Service, provides database instances – **Dependent on the Exchange System Attendant Resource**
 - ◆ Exchange Message Transfer Agent Instance – MTA Resource; represents the MTA service, responsible for legacy message transfer – **Dependent on the Exchange System Attendant resource**

- ◆ Exchange Routing Service Instance – Exchange Routing Service Resource; represents the routing service – **Dependent on the Exchange System Attendant resource**
 - ◆ Exchange SMTP Virtual Server Instance 1 – SMTP Service – **Dependent on the Exchange System Attendant resource**
 - ◆ Exchange HTTP Virtual Server Instance 100 – HTTP Virtual Server; provides WebDAV and OWA – **Dependent on the Exchange System Attendant resource**
 - ◆ Exchange POP3 Virtual Server Instance – POP3 Service; – **Dependent on the Exchange System Attendant resource**
 - ◆ Exchange IMAP4 Virtual Server Instance – IMAP4 Virtual Server – **Dependent on the Exchange System Attendant resource**
 - ◆ DTCONN-SITE2 – Double-Take Source Connection; Double-Take replication provider to Sterling – **Dependent on ALL physical Disk Resources**
 - ◆ DTCONN-SITE3 – Double-Take Source connection; Double-Take replication provider to Atlanta – **Dependent on ALL Physical Disk Resources**
- **NIHCESMLBXHA2 (Exchange Virtual Server)**
- NIHCESMLBXHA2A – Physical Server Node (156.40.71.144)
 - NIHCESMLBXHA2B – Physical Server Node (156.40.71.145)
 - **NIHCESCLUSTER2 Default Cluster Group** – Defines the cluster object, and contains the following resources:
 - ◆ Disk Q: (Quorum) – Cluster object Physical Disk resource; used as the Quorum disk, storing the definitive copy of the cluster configuration so that regardless of failures, the cluster configuration remains consistent – No dependencies
 - ◆ Cluster IP Address (156.40.71.146) – Cluster object IP Address Resource; used by the cluster service and cluster management utilities to manage the cluster groups and resources – no dependencies
 - ◆ Cluster Name (NIHCESCLUSTER2) – Cluster object NetBIOS Resource; used by the cluster service and cluster management utilities to manage the cluster groups and resources – **Dependent on the Cluster IP Address Resource**
 - ◆ Distributed Transaction Coordinator – Cluster object MS-DTC resource; required by Exchange Server 2003 clusters, but should be owned by the default cluster group, not the Exchange Virtual Server – **Dependent on the Quorum Disk, IP Address, and Network Name resources**
 - **CES-EVS-2** – Exchange Virtual Server, contains the following Resources:
 - ◆ Exchange SG1 LOGS Disk G: - Physical Disk Resource; Location of SG1 Log Files – No Dependencies
 - ◆ Exchange SG2 LOGS Disk H: - Physical Disk Resource; Location of SG2 Log Files – No Dependencies
 - ◆ Exchange SG3 LOGS Disk I: - Physical Disk Resource; Location of SG3 Log Files – No Dependencies

- ◆ Exchange SG4 LOGS Disk J: - Physical Disk Resource; Location of SG4 Log Files – No Dependencies
- ◆ Exchange MTA/SMTP Disk N: - Physical Disk Resource; Location of MTA and SMTP Virtual Server Queue Directories – No Dependencies
- ◆ Exchange SG1 DATA Disk R: - Physical Disk Resource; Location of SG1 Database Files – No Dependencies
- ◆ Exchange SG2 DATA Disk S: - Physical Disk Resource; Location of SG2 Database Files – No Dependencies
- ◆ Exchange SG3 DATA Disk T: - Physical Disk Resource; Location of SG3 Database Files – No Dependencies
- ◆ Exchange SG4 DATA Disk U: - Physical Disk Resource; Location of SG4 Database Files – No Dependencies
- ◆ Exchange IP Address (156.40.71.147) – IP Address Resource of the Exchange Virtual Server; registered on the **PUBLIC** interface – No Dependencies
- ◆ Exchange Network Name (NIHCESMLBXHA2) – NetBIOS Network Name Resource; this resource represents the Exchange Server listed in the Exchange System Manager, and is the Exchange Server name clients connect to, it is bound to the Exchange IP Address and must register in DNS in order for the cluster service to bring it online – **Dependent on the Exchange Network Name Resource**
- ◆ Exchange System Attendant – Exchange System Attendant Resource; bound to the **Exchange Network Name** resource; represents the Exchange System Attendant Service for the Exchange Virtual Server – **Dependent on Exchange Network Name Resource and ALL Physical Disk Resources**
- ◆ Exchange Information Store Instance – Information Store Resource; represents the Information Store Service, provides database instances – **Dependent on the Exchange System Attendant Resource**
- ◆ Exchange Message Transfer Agent Instance – MTA Resource; represents the MTA service, responsible for legacy message transfer – **Dependent on the Exchange System Attendant resource**
- ◆ Exchange Routing Service Instance – Exchange Routing Service Resource; represents the routing service – **Dependent on the Exchange System Attendant resource**
- ◆ Exchange SMTP Virtual Server Instance 1 – SMTP Service – **Dependent on the Exchange System Attendant resource**
- ◆ Exchange HTTP Virtual Server Instance 100 – HTTP Virtual Server; provides WebDAV and OWA – **Dependent on the Exchange System Attendant resource**
- ◆ Exchange POP3 Virtual Server Instance – POP3 Service; – **Dependent on the Exchange System Attendant resource**
- ◆ Exchange IMAP4 Virtual Server Instance – IMAP4 Virtual Server – **Dependent on the Exchange System Attendant resource**
- ◆ DTCONN-SITE2 – Double-Take Source Connection; Double-Take replication provider to Sterling – **Dependent on ALL physical Disk Resources**

- ◆ DTCONN-SITE3 – Double-Take Source connection; Double-Take replication provider to Atlanta – **Dependent on ALL Physical Disk Resources**

SITE 2 (Sterling) Cluster Configuration

Two (2) MSCS Server Clusters on Windows Server 2003 SP2 Enterprise Edition. Each is an Exchange Server 2003 SP2 Enterprise Edition Mailbox Server single-node Cluster. Each cluster consists of two cluster groups, the **NIHCESCLUSTERxx Default Cluster Group**, and the Exchange Virtual Server group, **CES-EVS-x-x**. Each cluster node has one network card installed, being used for both **PUBLIC NETWORK** and **PRIVATE CLUSTER** communications.

Each Server Node has at least four (3) IP addresses:

- Physical node IP address
- Cluster IP Address
- Exchange Virtual Server IP Address

All resources in a cluster group can only be owned or active on one node at a time. In the event of a problem with that node, the cluster service will move those resources to the other node automatically. The cluster service owns and manages all cluster resources, so any changes that need to be made to those resources should be done using the Cluster Admin utility (i.e. – To stop the SMTP Service, you use the Cluster Admin utility to take the Exchange SMTP Virtual Server Instance 1 offline).

- **NIHMLBXHAR21 (Exchange Virtual Server)**
 - NIHMLBXHAR21A – Physical Server Node (165.112.1.150)
 - **NIHCESCLUSTER21 Default Cluster Group** – Defines the cluster object, and contains the following resources:
 - ◆ Disk Q: (Quorum) – Cluster object Physical Disk resource; used as the Quorum disk, storing the definitive copy of the cluster configuration so that regardless of failures, the cluster configuration remains consistent – No dependencies
 - ◆ Cluster IP Address (165.112.1.151) – Cluster object IP Address Resource; used by the cluster service and cluster management utilities to manage the cluster groups and resources – no dependencies
 - ◆ Cluster Name (NIHCESCLUSTER21) – Cluster object NetBIOS Resource; used by the cluster service and cluster management utilities to manage the cluster groups and resources – **Dependent on the Cluster IP Address Resource**
 - ◆ Distributed Transaction Coordinator – Cluster object MS-DTC resource; required by Exchange Server 2003 clusters, but should be owned by the default cluster group, not the Exchange Virtual Server – **Dependent on the Quorum Disk, IP Address, and Network Name resources**
 - **CES-EVS-2-2** – Exchange Virtual Server, contains the following Resources:

- ◆ Exchange SG1 LOGS Disk G: - Physical Disk Resource; Location of SG1 Log Files – No Dependencies
- ◆ Exchange SG2 LOGS Disk H: - Physical Disk Resource; Location of SG2 Log Files – No Dependencies
- ◆ Exchange SG3 LOGS Disk I: - Physical Disk Resource; Location of SG3 Log Files – No Dependencies
- ◆ Exchange SG4 LOGS Disk J: - Physical Disk Resource; Location of SG4 Log Files – No Dependencies
- ◆ Exchange MTA/SMTP Disk N: - Physical Disk Resource; Location of MTA and SMTP Virtual Server Queue Directories – No Dependencies
- ◆ Exchange SG1 DATA Disk R: - Physical Disk Resource; Location of SG1 Database Files – No Dependencies
- ◆ Exchange SG2 DATA Disk S: - Physical Disk Resource; Location of SG2 Database Files – No Dependencies
- ◆ Exchange SG3 DATA Disk T: - Physical Disk Resource; Location of SG3 Database Files – No Dependencies
- ◆ Exchange SG4 DATA Disk U: - Physical Disk Resource; Location of SG4 Database Files – No Dependencies
- ◆ Exchange IP Address (165.112.1.155) – IP Address Resource of the Exchange Virtual Server; registered on the **PUBLIC** interface – No Dependencies
- ◆ Exchange Network Name (NIHMLBXHAR22) – NetBIOS Network Name Resource; this resource represents the Exchange Server listed in the Exchange System Manager, and is the Exchange Server name clients connect to, it is bound to the Exchange IP Address and must register in DNS in order for the cluster service to bring it online – **Dependent on the Exchange Network Name Resource**
- ◆ Exchange System Attendant – Exchange System Attendant Resource; bound to the **Exchange Network Name** resource; represents the Exchange System Attendant Service for the Exchange Virtual Server – **Dependent on Exchange Network Name Resource and ALL Physical Disk Resources**
- ◆ Exchange Information Store Instance – Information Store Resource; represents the Information Store Service, provides database instances – **Dependent on the Exchange System Attendant Resource**
- ◆ Exchange Message Transfer Agent Instance – MTA Resource; represents the MTA service, responsible for legacy message transfer – **Dependent on the Exchange System Attendant resource**
- ◆ Exchange Routing Service Instance – Exchange Routing Service Resource; represents the routing service – **Dependent on the Exchange System Attendant resource**
- ◆ Exchange SMTP Virtual Server Instance 1 – SMTP Service – **Dependent on the Exchange System Attendant resource**
- ◆ Exchange HTTP Virtual Server Instance 100 – HTTP Virtual Server; provides WebDAV and OWA – **Dependent on the Exchange System Attendant resource**

- ◆ Exchange POP3 Virtual Server Instance – POP3 Service; – **Dependent on the Exchange System Attendant resource**
- ◆ Exchange IMAP4 Virtual Server Instance – IMAP4 Virtual Server – **Dependent on the Exchange System Attendant resource**

SITE 3 (Atlanta) Cluster Configuration

Two (2) MSCS Server Clusters on Windows Server 2003 SP2 Enterprise Edition. Each is an Exchange Server 2003 SP2 Enterprise Edition Mailbox Server single-node Cluster. Each cluster consists of two cluster groups, the **NIHCESCLUSTRxx Default Cluster Group**, and the Exchange Virtual Server group, **CES-EVS-x-x**. Each cluster node has one network card installed, being used for both **PUBLIC NETWORK** and **PRIVATE CLUSTER** communications.

Each Server Node has at least four (3) IP addresses:

- Physical node IP address
- Cluster IP Address
- Exchange Virtual Server IP Address

All resources in a cluster group can only be owned or active on one node at a time. In the event of a problem with that node, the cluster service will move those resources to the other node automatically. The cluster service owns and manages all cluster resources, so any changes that need to be made to those resources should be done using the Cluster Admin utility (i.e. – To stop the SMTP Service, you use the Cluster Admin utility to take the Exchange SMTP Virtual Server Instance 1 offline).

➤ **NIHMLBXHAR31 (Exchange Virtual Server)**

- NIHMLBXHAR31A – Physical Server Node (158.74.255.80)
 - **NIHCESCLUSTR31 Default Cluster Group** – Defines the cluster object, and contains the following resources:
 - ◆ Disk Q: (Quorum) – Cluster object Physical Disk resource; used as the Quorum disk, storing the definitive copy of the cluster configuration so that regardless of failures, the cluster configuration remains consistent – No dependencies
 - ◆ Cluster IP Address (158.74.255.81) – Cluster object IP Address Resource; used by the cluster service and cluster management utilities to manage the cluster groups and resources – no dependencies
 - ◆ Cluster Name (NIHCESCLUSTR31) – Cluster object NetBIOS Resource; used by the cluster service and cluster management utilities to manage the cluster groups and resources – **Dependent on the Cluster IP Address Resource**
 - ◆ Distributed Transaction Coordinator – Cluster object MS-DTC resource; required by Exchange Server 2003 clusters, but should be owned by the default cluster group, not the Exchange Virtual Server – **Dependent on the Quorum Disk, IP Address, and Network Name resources**

- **CES-EVS-3-1** – Exchange Virtual Server, contains the following Resources:
 - ◆ Exchange SG1 LOGS Disk G: - Physical Disk Resource; Location of SG1 Log Files – No Dependencies
 - ◆ Exchange SG2 LOGS Disk H: - Physical Disk Resource; Location of SG2 Log Files – No Dependencies
 - ◆ Exchange SG3 LOGS Disk I: - Physical Disk Resource; Location of SG3 Log Files – No Dependencies
 - ◆ Exchange SG4 LOGS Disk J: - Physical Disk Resource; Location of SG4 Log Files – No Dependencies
 - ◆ Exchange MTA/SMTP Disk N: - Physical Disk Resource; Location of MTA and SMTP Virtual Server Queue Directories – No Dependencies
 - ◆ Exchange SG1 DATA Disk R: - Physical Disk Resource; Location of SG1 Database Files – No Dependencies
 - ◆ Exchange SG2 DATA Disk S: - Physical Disk Resource; Location of SG2 Database Files – No Dependencies
 - ◆ Exchange SG3 DATA Disk T: - Physical Disk Resource; Location of SG3 Database Files – No Dependencies
 - ◆ Exchange SG4 DATA Disk U: - Physical Disk Resource; Location of SG4 Database Files – No Dependencies
 - ◆ Exchange IP Address (158.74.255.82) – IP Address Resource of the Exchange Virtual Server; registered on the **PUBLIC** interface – No Dependencies
 - ◆ Exchange Network Name (NIHMLBXHAR31) – NetBIOS Network Name Resource; this resource represents the Exchange Server listed in the Exchange System Manager, and is the Exchange Server name clients connect to, it is bound to the Exchange IP Address and must register in DNS in order for the cluster service to bring it online – **Dependent on the Exchange Network Name Resource**
 - ◆ Exchange System Attendant – Exchange System Attendant Resource; bound to the **Exchange Network Name** resource; represents the Exchange System Attendant Service for the Exchange Virtual Server – **Dependent on Exchange Network Name Resource and ALL Physical Disk Resources**
 - ◆ Exchange Information Store Instance – Information Store Resource; represents the Information Store Service, provides database instances – **Dependent on the Exchange System Attendant Resource**
 - ◆ Exchange Message Transfer Agent Instance – MTA Resource; represents the MTA service, responsible for legacy message transfer – **Dependent on the Exchange System Attendant resource**
 - ◆ Exchange Routing Service Instance – Exchange Routing Service Resource; represents the routing service – **Dependent on the Exchange System Attendant resource**
 - ◆ Exchange SMTP Virtual Server Instance 1 – SMTP Service – **Dependent on the Exchange System Attendant resource**
 - ◆ Exchange HTTP Virtual Server Instance 100 – HTTP Virtual Server; provides WebDAV and OWA – **Dependent on the Exchange System Attendant resource**

- ◆ Exchange POP3 Virtual Server Instance – POP3 Service; – **Dependent on the Exchange System Attendant resource**
- ◆ Exchange IMAP4 Virtual Server Instance – IMAP4 Virtual Server – **Dependent on the Exchange System Attendant resource**
- **NIHMLBXHAR32 (Exchange Virtual Server)**
 - NIHMLBXHAR32A – Physical Server Node (158.74.255.83)
 - **NIHCESCLUSTER21 Default Cluster Group** – Defines the cluster object, and contains the following resources:
 - ◆ Disk Q: (Quorum) – Cluster object Physical Disk resource; used as the Quorum disk, storing the definitive copy of the cluster configuration so that regardless of failures, the cluster configuration remains consistent – No dependencies
 - ◆ Cluster IP Address (158.74.255.84) – Cluster object IP Address Resource; used by the cluster service and cluster management utilities to manage the cluster groups and resources – no dependencies
 - ◆ Cluster Name (NIHCESCLUSTER21) – Cluster object NetBIOS Resource; used by the cluster service and cluster management utilities to manage the cluster groups and resources – **Dependent on the Cluster IP Address Resource**
 - ◆ Distributed Transaction Coordinator – Cluster object MS-DTC resource; required by Exchange Server 2003 clusters, but should be owned by the default cluster group, not the Exchange Virtual Server – **Dependent on the Quorum Disk, IP Address, and Network Name resources**
 - **CES-EVS-2-1** – Exchange Virtual Server, contains the following Resources:
 - ◆ Exchange SG1 LOGS Disk G: - Physical Disk Resource; Location of SG1 Log Files – No Dependencies
 - ◆ Exchange SG2 LOGS Disk H: - Physical Disk Resource; Location of SG2 Log Files – No Dependencies
 - ◆ Exchange SG3 LOGS Disk I: - Physical Disk Resource; Location of SG3 Log Files – No Dependencies
 - ◆ Exchange SG4 LOGS Disk J: - Physical Disk Resource; Location of SG4 Log Files – No Dependencies
 - ◆ Exchange MTA/SMTP Disk N: - Physical Disk Resource; Location of MTA and SMTP Virtual Server Queue Directories – No Dependencies
 - ◆ Exchange SG1 DATA Disk R: - Physical Disk Resource; Location of SG1 Database Files – No Dependencies
 - ◆ Exchange SG2 DATA Disk S: - Physical Disk Resource; Location of SG2 Database Files – No Dependencies
 - ◆ Exchange SG3 DATA Disk T: - Physical Disk Resource; Location of SG3 Database Files – No Dependencies
 - ◆ Exchange SG4 DATA Disk U: - Physical Disk Resource; Location of SG4 Database Files – No Dependencies
 - ◆ Exchange IP Address (158.74.255.85) – IP Address Resource of the Exchange Virtual Server; registered on the **PUBLIC** interface – No Dependencies

- ◆ Exchange Network Name (NIHMLBXHAR32) – NetBIOS Network Name Resource; this resource represents the Exchange Server listed in the Exchange System Manager, and is the Exchange Server name clients connect to, it is bound to the Exchange IP Address and must register in DNS in order for the cluster service to bring it online – **Dependent on the Exchange Network Name Resource**
- ◆ Exchange System Attendant – Exchange System Attendant Resource; bound to the **Exchange Network Name** resource; represents the Exchange System Attendant Service for the Exchange Virtual Server – **Dependent on Exchange Network Name Resource and ALL Physical Disk Resources**
- ◆ Exchange Information Store Instance – Information Store Resource; represents the Information Store Service, provides database instances – **Dependent on the Exchange System Attendant Resource**
- ◆ Exchange Message Transfer Agent Instance – MTA Resource; represents the MTA service, responsible for legacy message transfer – **Dependent on the Exchange System Attendant resource**
- ◆ Exchange Routing Service Instance – Exchange Routing Service Resource; represents the routing service – **Dependent on the Exchange System Attendant resource**
- ◆ Exchange SMTP Virtual Server Instance 1 – SMTP Service – **Dependent on the Exchange System Attendant resource**
- ◆ Exchange HTTP Virtual Server Instance 100 – HTTP Virtual Server; provides WebDAV and OWA – **Dependent on the Exchange System Attendant resource**
- ◆ Exchange POP3 Virtual Server Instance – POP3 Service; – **Dependent on the Exchange System Attendant resource**
- ◆ Exchange IMAP4 Virtual Server Instance – IMAP4 Virtual Server – **Dependent on the Exchange System Attendant resource**

Exchange Data Replication Configuration

The NIH CES has chosen to use a host-based replication utility to provide replication for Exchange Databases containing the DR server users. This will allow users to have access to all items in their mailbox at the time a failover is deemed necessary. Replication is being provided by Double-Take Standard Edition for Windows 200x Advanced Server, from Double-Take Software. Double-Take Standard Edition is installed on all eight (8) Exchange Mailbox server nodes in the DR deployment. Double-Take was chosen over other competitive products for two primary reasons:

1. Double-Take is a true cluster-aware application. This means that Double_take creates a cluster resource type that can be defined in the Cluster Administrator program, allowing the Double-Take connections to failover between nodes in each cluster. The benefit of this is that allows for replication to resume in the event of a cluster node failure without the need for a “re-mirror” process. The status of replicated data is available to all cluster nodes.

2. Double-Take also provides a Microsoft Operations Management Server (MOM) Management Pack for the purpose of monitoring the Double-Take application. The NIH CES uses MOM for monitoring of all Exchange Systems, so this capability has immediate benefit by allowing CES to enable monitoring using existing CES processes.

➤ **NIHCESMLBXHA**

- NIHCESMLBXHA1A (Exchange Mailbox Server Cluster Node)
- NIHCESMLBXHA1B (Exchange Mailbox Server Cluster Node)
 - NIHCESMLBXHA-REP-SET (Double-Take Replication Set)
 - ◆ Defines all Exchange Logs/Databases and SMTP/MTA directories to be replicated from the host systems in Bethesda (SITE1) to SITE2 and SITE3
 - DTCONN-SITE2
 - ◆ Double-Take Source connection Clustered resource
 - ◆ Manages Connection between Bethesda and Sterling
 - ◆ While this resource is online (in Cluster Admin), Exchange data is being replicated from NIHCESMLBXHA to NIHMLBXHAR21 in near real-time
 - ◆ Replication is at the byte-level
 - DTCONN-SITE3
 - ◆ Double-Take Source connection Clustered resource
 - ◆ Manages Connection between Bethesda and Atlanta
 - ◆ While this resource is online (in Cluster Admin), Exchange data is being replicated from NIHCESMLBXHA to NIHMLBXHAR31 in near real-time
 - ◆ Replication is at the byte-level

➤ **NIHCESMLBXHA2**

- NIHCESMLBXHA2A (Exchange Mailbox Server Cluster Node)
- NIHCESMLBXHA2B (Exchange Mailbox Server Cluster Node)
 - NIHCESMLBXHA2-REP-SET (Double-Take Replication Set)
 - ◆ Defines all Exchange Logs/Databases and SMTP/MTA directories to be replicated from the host systems in Bethesda (SITE1) to SITE2 and SITE3
 - DTCONN-SITE2
 - ◆ Double-Take Source connection Clustered resource
 - ◆ Manages Connection between Bethesda and Sterling
 - ◆ While this resource is online (in Cluster Admin), Exchange data is being replicated from NIHCESMLBXHA2 to NIHMLBXHAR22 in near real-time
 - ◆ Replication is at the byte-level
 - DTCONN-SITE3
 - ◆ Double-Take Source connection Clustered resource
 - ◆ Manages Connection between Bethesda and Atlanta
 - ◆ While this resource is online (in Cluster Admin), Exchange data is being replicated from NIHCESMLBXHA2 to NIHMLBXHAR32 in near real-time
 - ◆ Replication is at the byte-level

Double-Take connection(s) exist only on the Primary servers in Bethesda. The reason for this is that connections are made and maintained from Source-to-Target. Double-Take is installed on the Exchange mailbox servers in the Site's 2 & 3 so they can be configured as replication targets, and so they can replicate post-failover data back to Site 1 for failback purposes.

Procedure for Executing Exchange Failover Following a Primary Site Failure

1. NIH and/or CIT management determines the scope of the Primary Site failure and invokes Disaster Recovery Operations for NIH Messaging
2. EMIB Branch Chief activates CES Messaging Team and instructs to bring Site x online
3. CES messaging team member connects to NIH VPN solution, and then uses Terminal Services to connect to **NIHMLBXHRx1 & NIHMLBXHRx2**
4. Open a command prompt on **NIHMLBXHRx1**
5. Change directory to C:\program Files\Doubletake
6. Execute **post_failover_NIHCESMLBXHRx1_NIHMLBXHRx1.bat**
 - 6.1. This batch file performs the following steps:
 - 6.1.1. Runs the DNS Failover utility to update the DNS record(s) for the source server and point them to the target server
 - 6.1.2. flushes the DNS cache
 - 6.1.3. Pauses failover so the target replication queue can empty
 - 6.1.4. Uses the Exchange Failover utility to setup the target databases for failover (sets the flag that the databases can be overwritten by a restore; this allows the databases to mount on the target)
 - 6.1.5. Starts the Exchange Cluster Resource Services on the Target
 - 6.1.6. Runs the Exchange Failover utility to move users to the target server
 - 6.1.6.1.Updates the SPN of the Exchange host
 - 6.1.6.2.Updates the homeMDB attribute of users in the databases
 - 6.1.6.3.Updates the homeMTA attribute of users in the databases
 - 6.1.6.4.Updates the MsExchHomeServerName attribute of users in the databases
 - 6.1.7. Sets the failover state to be persistent in the event of failover within the target cluster
7. Open a command prompt on **NIHMLBXHRx2**
8. Change directory to C:\Program Files\Doubletake
9. Execute **post_failover_NIHCESMLBXHRx2_NIHMLBXHRx2.bat**
 - 9.1. This batch file performs the following steps:
 - 9.1.1. Runs the DNS Failover utility to update the DNS record(s) for the source server and point them to the target server
 - 9.1.2. flushes the DNS cache
 - 9.1.3. Pauses failover so the target replication queue can empty
 - 9.1.4. Uses the Exchange Failover utility to setup the target databases for failover (sets the flag that the databases can be overwritten by a restore; this allows the databases to mount on the target)
 - 9.1.5. Starts the Exchange Cluster Resource Services on the Target
 - 9.1.6. Runs the Exchange Failover utility to move users to the target server
 - 9.1.6.1.Updates the SPN of the Exchange host
 - 9.1.6.2.Updates the homeMDB attribute of users in the databases

- 9.1.6.3.Updates the homeMTA attribute of users in the databases
- 9.1.6.4.Updates the MsExchHomeServerName attribute of users in the databases
- 9.1.7. Sets the failover state to be persistent in the event of failover within the target cluster
- 10. Allow ~30 minutes for Active Directory Replication
- 11. Customers homed on the DR servers can access their mailbox via OWA

Procedure for Executing Failback to Primary Data Center

If a disaster is declared, and Exchange Failover to one of the remote sites is invoked, it is assumed that the Primary data Center will eventually be brought back online. Once the Primary Data Center is back online, a procedure will need to be performed to initiate failback. This should be done during off-hours to minimize user disruption and limit the amount of changes trying to be made to the Exchange databases

1. Verify the **NIHCESMLBXHA** & **NIHCESMLBXHA2**, are available, and the appropriate version of Exchange server is installed, but not running.
2. Login to **NIHMLBXHARx1** & **NIHMLBXHARx2** using Terminal Services
3. Open a command prompt
4. Change Directory to **C:\Program Files\Doubletake**
5. Run the **pre_failback_NIHCESMLBXHA_NIHMLBXHARx1.bat** from **NIHMLBXHARx1** and **pre_failback_NIHCESMLBXHA2_NIHMLBXHARx2.bat** from **NIHMLBXHARx2**
 - 5.1. This takes Exchange on the Target/Remote Server offline so changes are not being made to the Exchange databases
6. Start the **Double-Take Management Console** on **NIHMLBXHARx1** & **NIHMLBXHARx2**
 - 6.1. There should not be an existing connection, but if there is, right-click it and choose **Disconnect**
7. Select **Tools>Restoration Manager**
8. Complete the fields in the **Restoration Manager**
 - 8.1. **Original Source** – IP of the Source Exchange Server (Physical Node)
 - 8.2. **Restore From** – The Target server containing the updated Exchange data (i.e. **NIHMLBXHARx1**)
 - 8.3. **Replication Set** – This may need to be defined
 - 8.4. **Restore To** – IP of the Source Exchange Server (Physical Node)
9. Disable **Only if backup copy is more recent** option
10. Click the **Orphans** tab
11. Select **Move or delete orphan files on the source**
12. Click **Restore**
13. Once the data restoration has been completed, login to the **NIHCESMLBXHA1A** & **NIHCESMLBXHA2A** servers using Terminal Services
14. Open a command prompt on each server
15. Change directory to **C:\Program Files\DoubleTake**
16. Execute **post_restore_NIHCESMLBXHA_NIHMLBXHARx1.bat** from **NIHCESMLBXHA1A**

17. Execute **post_restore_NIHCESMLBXHA2_NIHMLBXHARx2.bat** from **NIHCESMLBXHA2A**
18. Once the scripts complete and Active Directory Replication has completed, users will be able to access their mailboxes on the original server

November 05, 2008